DOC 54 **2512/001**

BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS

8 juni 2017

WETSONTWERP

inzake elektronische identificatie

CHAMBRE DES REPRÉSENTANTS DE BELGIQUE

8 juin 2017

PROJET DE LOI

relatif à l'identification électronique

Blz.

INHOUD

Pages

SOMMAIRE

DE SPOEDBEHANDELING WORDT DOOR DE REGERING GEVRAAGD OVEREENKOMSTIG ARTIKEL 51 VAN HET REGLEMENT.

LE GOUVERNEMENT DEMANDE L'URGENCE CONFORMÉMENT À L'ARTICLE 51 DU RÈGLEMENT.

De regering heeft dit wetsontwerp op 8 juni 2017 ingediend.	*Le gouvernement a déposé ce projet de loi le 8 juin 2017.*
De "goedkeuring tot drukken" werd op 12 juni 2017 door de Kamer ontvangen.	*Le "bon à tirer" a été reçu à la Chambre le 12 juin 2017.*

N-VA	:	*Nieuw-Vlaamse Alliantie*
PS	:	*Parti Socialiste*
MR	:	*Mouvement Réformateur*
CD&V	:	*Christen-Democratisch en Vlaams*
Open Vld	:	*Open Vlaamse liberalen en democraten*
sp.a	:	*socialistische partij anders*
Ecolo-Groen	:	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
cdH	:	*centre démocrate Humaniste*
VB	:	*Vlaams Belang*
PTB-GO!	:	*Parti du Travail de Belgique – Gauche d'Ouverture*
DéFI	:	*Démocrate Fédéraliste Indépendant*
PP	:	*Parti Populaire*
Vuye&Wouters	:	*Vuye&Wouters*

Afkortingen bij de nummering van de publicaties:		*Abréviations dans la numérotation des publications:*	
DOC 54 0000/000:	*Parlementair document van de 54e zittingsperiode + basisnummer en volgnummer*	*DOC 54 0000/000:*	*Document parlementaire de la 54e législature, suivi du n° de base et du n° consécutif*
QRVA:	*Schriftelijke Vragen en Antwoorden*	*QRVA:*	*Questions et Réponses écrites*
CRIV:	*Voorlopige versie van het Integraal Verslag*	*CRIV:*	*Version Provisoire du Compte Rendu intégral*
CRABV:	*Beknopt Verslag*	*CRABV:*	*Compte Rendu Analytique*
CRIV:	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaald beknopt verslag van de toespraken (met de bijlagen)*	*CRIV:*	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)*
PLEN:	*Plenum*	*PLEN:*	*Séance plénière*
COM:	*Commissievergadering*	*COM:*	*Réunion de commission*
MOT:	*Moties tot besluit van interpellaties (beigekleurig papier)*	*MOT:*	*Motions déposées en conclusion d'interpellations (papier beige)*

Officiële publicaties, uitgegeven door de Kamer van volksvertegenwoordigers

Bestellingen:
Natieplein 2
1008 Brussel
Tel. : 02/ 549 81 60
Fax : 02/549 82 74
www.dekamer.be
e-mail : publicaties@dekamer.be

De publicaties worden uitsluitend gedrukt op FSC gecertificeerd papier

Publications officielles éditées par la Chambre des représentants

Commandes:
Place de la Nation 2
1008 Bruxelles
Tél. : 02/ 549 81 60
Fax : 02/549 82 74
www.lachambre.be
courriel : publications@lachambre.be

Les publications sont imprimées exclusivement sur du papier certifié FSC

SAMENVATTING

Dit ontwerp van wet betreft enerzijds bepalingen die ervoor zorgen dat de verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, hoofdstuk II aangaande elektronische identificatie, volledige uitwerking kan hebben in België. Omdat de verordening rechtstreeks toepasselijk is in de lidstaten betreft het enkel bepalingen die het mogelijk moeten maken de verordening volledig tenuitvoer te leggen. Dit gedeelte van het ontwerp betreft elektronische identificatie in de Europese grensoverschrijdende context.

Dit ontwerp van wet strekt er anderzijds toe om een juridisch kader te creëren voor elektronische identificatie voor digitale overheidstoepassingen in België. In het bijzonder voorziet dit ontwerp in een wettelijke verankering van de authenticatiedienst "FAS" en in de mogelijkheid om diensten voor elektronische identificatie te erkennen met het oog op het verlenen van toegang tot Belgische overheidstoepassingen binnen de authenticatiedienst. Dit gedeelte van het ontwerp betreft elektronische identificatie in de Belgische context.

RÉSUMÉ

Le présent projet de loi porte d'une part sur les dispositions permettant au règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, chapitre II portant sur l'identification électronique, de sortir tous ses effets en Belgique. Comme le règlement est directement applicable dans les États membres, il ne s'agit que des dispositions qui doivent permettre la pleine mise en œuvre du règlement. Cette partie du projet concerne l'identification électronique dans le contexte transfrontalier européen.

Le présent projet de loi vise d'autre part à créer un cadre juridique pour l'identification électronique sur des applications publiques numériques en Belgique. Ce projet prévoit en particulier l'ancrage légal du service d'authentification "FAS" et la possibilité d'agréer des services d'identification électronique afin d'octroyer l'accès à des applications publiques belges au sein du service d'authentification. Cette partie du projet concerne l'identification électronique dans le contexte belge.

MEMORIE VAN TOELICHTING

DAMES EN HEREN,

A. **ALGEMENE TOELICHTING**

Het huidige ontwerp kadert in het globale e-governmentbeleid van de regering. *E-government* of "elektronische administratie" omvat het uitbouwen van een informaticastructuur en het nemen van initiatieven om administraties, burgers en ondernemingen in staat te stellen de informatie- en communicatietechnologie te gebruiken voor digitale overheidstoepassingen. Bovendien past het ontwerp in de digitale agenda van België omdat het op deze manier innovatie wil stimuleren en ondersteunen.

Een essentiële bouwsteen binnen e-government is de elektronische identificatie van burgers en ondernemingen.

Om deel te nemen aan *e-government* dienen burgers en ondernemingen zich online te kunnen identificeren, authentiseren en aanmelden voor overheidstoepassingen. Ze hebben nood aan mogelijkheden om hun identiteit ook online makkelijk te kunnen bewijzen.

Dit ontwerp van wet zorgt er enerzijds voor dat verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (hierna verordening 910/2014), voor wat betreft hoofdstuk II aangaande elektronische identificatie, volledige uitwerking kan hebben.

Anderzijds strekt dit ontwerp van wet ertoe de Belgische federale authenticatiedienst wettelijk te verankeren en mogelijkheden te voorzien om diensten voor elektronische identificatie te erkennen met het oog op het verlenen van toegang tot Belgische overheidstoepassingen.

B. **TOEPASSING HOOFDSTUK II VERORDENING 910/2014**

Op 23 juli 2014 keurde de Europese wetgever verordening 910/2014 goed.

De hoofddoelstelling van die verordening is de invoering van een juridisch kader om het vertrouwen in elektronische transacties in de interne markt te vergroten. Deze verordening trekt de Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor

EXPOSÉ DES MOTIFS

MESDAMES, MESSIEURS,

A. **EXPOSÉ GÉNÉRAL**

Le présent projet s'inscrit dans la politique d'e-gouvernement globale du gouvernement. L'e-gouvernement ou "administration électronique" recouvre le développement d'une structure informatique et la prise d'initiatives afin de permettre aux administrations, aux citoyens et aux entreprises d'utiliser les technologies de l'information et de la communication dans le cadre d'applications publiques numériques. En outre, le projet s'inscrit dans le cadre de l'agenda numérique de la Belgique étant donné qu'il entend ainsi stimuler et soutenir l'innovation.

Un fondement essentiel de l'e-gouvernement est l'identification électronique des citoyens et des entreprises.

Pour participer à l'e-gouvernement, les citoyens et les entreprises doivent pouvoir s'identifier, s'authentifier et se connecter en ligne sur des applications publiques. Ils ont besoin de méthodes leur permettant de prouver facilement leur identité en ligne.

Le présent projet de loi permet d'une part au règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (dénommé ci-après "règlement 910/2014"), concernant le chapitre II portant sur l'identification électronique, de sortir tous ses effets.

Le présent projet de loi vise d'autre part à ancrer légalement le service fédéral d'authentification belge et à prévoir des possibilités pour agréer des services d'identification électronique afin d'accéder à des applications publiques belges.

B. **APPLICATION DU CHAPITRE II DU RÈGLEMENT 910/2014**

Le 23 juillet 2014, le législateur européen a approuvé le règlement 910/2014.

L'objectif principal de ce règlement est d'instaurer un cadre juridique afin d'accroître la confiance dans les transactions électroniques du marché intérieur. Ce règlement abroge la Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques

elektronische handtekeningen in maar neemt niettemin het merendeel van haar bepalingen over. Hiertoe worden enkele wijzigingen aangebracht en worden een aantal nieuwe bepalingen toegevoegd. Deze bepalingen hebben enerzijds betrekking op de wederzijdse erkenning op Europees niveau van de aangemelde stelsels voor elektronische identificatie en anderzijds op de vertrouwensdiensten voor elektronische handtekeningen, voor elektronische zegels, voor elektronische tijdstempels, voor elektronisch aangetekende bezorging alsook voor websiteauthenticatie.

De verordening 910/2014 telt zes hoofdstukken. De twee belangrijkste hoofdstukken zijn het tweede hoofdstuk over de "elektronische identificatie" en het derde hoofdstuk over de "vertrouwensdiensten", omdat ze substantiële nieuwigheden op die beide gebieden bevatten. De andere vier hoofdstukken (die respectievelijk betrekking hebben op de algemene bepalingen, de elektronische documenten, de gedelegeerde handelingen, de uitvoeringshandelingen en de slotbepalingen) bevatten "bijkomende" bepalingen, hoofdzakelijk met het oog op de werking van de twee voornoemde hoofdstukken.

Hoofdstuk II van verordening 910/2014 over de "elektronische identificatie" is van directe toepassing in Belgisch recht maar een aantal wetsbepalingen op Belgisch niveau, zoals hierna in de artikelsgewijze commentaar verder toegelicht, dragen ertoe bij de door de overheid aangemelde stelsels voor elektronische identificatie, en het beheer daarvan, in lijn te brengen met de verplichtingen van verordening 910/2014.

Hoewel het merendeel van de bepalingen van hoofdstuk II van verordening 910/2014 reeds in werking zijn getreden, treedt de verplichting voor lidstaten tot wederzijdse erkenning van elektronische identificatiemiddelen maar in werking op 29 september 2018. Voor die datum kunnen lidstaten niettemin vrijwillig beslissen om bij de Commissie aangemelde stelsels te aanvaarden.

In deze context zorgt dit ontwerp van wet ervoor dat hoofdstuk II van verordening 910/2014 volledige uitwerking kan hebben. Daartoe wordt een wet betreffende elektronische identificatie aangenomen waarin onder andere wordt voorzien in bepalingen over de betrouwbaarheidsniveaus en over het toezichts- en controlemechanisme en concrete bepalingen omtrent samenwerking en interoperabiliteit.

mais reprend néanmoins la majorité de ses dispositions. À cette fin, quelques modifications sont apportées et une série de nouvelles dispositions sont ajoutées. Ces dispositions concernent d'une part la reconnaissance mutuelle au niveau européen des schémas d'identification électronique notifiés et d'autre part les services de confiance pour les signatures électroniques, pour les cachets électroniques, pour l'horodatage électronique, pour l'envoi recommandé électronique ainsi que pour authentification du site internet.

Le règlement 910/2014 comporte six chapitres. Le deuxième chapitre sur l'"identification électronique" et le troisième chapitre sur les "services de confiance" constituent les deux chapitres principaux, étant donné qu'ils comprennent des nouveautés substantielles dans ces deux domaines. Les quatre autres chapitres (qui concernent respectivement les dispositions générales, les documents électroniques, les délégations de pouvoir, les dispositions d'exécution et les dispositions finales) comprennent des dispositions "complémentaires", principalement en vue du fonctionnement des deux chapitres précités.

Le chapitre II du règlement 910/2014 consacré à l'"identification électronique" s'applique directement en droit belge mais une série de dispositions législatives au niveau belge, comme expliqué plus en détail ci-après dans le commentaire des articles, contribue à ce que les schémas d'identification électronique notifiés par l'Administration, et leur gestion, répondent aux obligations du règlement 910/2014.

Bien que la majorité des dispositions du chapitre II du règlement 910/2014 soient déjà entrées en vigueur, l'obligation pour les États membres de reconnaissance mutuelle des moyens d'identification électronique n'entrera en vigueur que le 29 septembre 2018. Avant cette date, les États membres peuvent néanmoins volontairement décider d'accepter les schémas notifiés à la Commission.

Dans ce contexte, le présent projet de loi permet au chapitre II du règlement 910/2014 de sortir tous ses effets. À cette fin, une loi relative à l'identification électronique est adoptée. Elle prévoit notamment des dispositions relatives aux niveaux de garantie, et au mécanisme de surveillance et de contrôle, ainsi que des dispositions concrètes portant sur la collaboration et l'interopérabilité.

C. **ELEKTRONISCHE IDENTIFICATIE VOOR BELGISCHE OVERHEIDSTOEPASSINGEN**

Het tweede gedeelte van het ontwerp heeft geen rechtstreekse link met de toepassing van verordening 910/2014, maar beoogt de invoering van een juridisch kader voor elektronische identificatie in de context van Belgische overheidstoepassingen.

Enerzijds betreft het de werking van de authenticatiedienst die identiteits- en toegangsbeheer doet voor overheidstoepassingen. Anderzijds voorziet het in de mogelijkheid om mobiele en niet mobiele elektronische identificatiemiddelen te erkennen die gebruikt kunnen worden om toegang te krijgen tot overheidstoepassingen. Daartoe wordt voorzien in de nodige bepalingen in deze wet betreffende elektronische identificatie.

D. **ARTIKELSGEWIJZE TOELICHTING**

HOOFDSTUK 1

Algemene bepaling

Artikel 1

Dit artikel vereist geen bijzondere commentaar.

HOOFDSTUK 2

Definities

Artikel 2

Artikel 2, § 1, 1° van dit ontwerp bepaalt dat als er sprake is van verordening 910/2014 men de verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, bedoelt. Immers, aangezien dit ontwerp ertoe strekt die verordening volledig ten uitvoer te leggen voor wat hoofdstuk II (elektronische identificatie) betreft, is het nuttig om die term te definieren, teneinde de tekst leesbaarder te maken, telkens wanneer verwezen wordt naar alle of een gedeelte van de bepalingen van de verordening. Hetzelfde geldt voor de uitvoeringsverordeningen van de verordening 910/2014 waarnaar verwezen wordt.

Artikel 2 § 1, 4° van dit ontwerp verwijst voor het begrip toezichthoudend orgaan naar artikel 6. Ook al wordt dit begrip in de verordening 910/2014 niet gehanteerd in de context van hoofdstuk II (elektronische identificatie),

C. **IDENTIFICATION ÉLECTRONIQUE POUR APPLICATIONS PUBLIQUES BELGES**

La seconde partie du projet n'a pas de lien direct avec l'application du règlement 910/2014 mais vise l'introduction d'un cadre juridique pour l'identification électronique dans le contexte des applications publiques belges.

Elle concerne d'une part le fonctionnement du service d'authentification qui se charge de la gestion de l'identité et de l'accès pour les applications publiques. D'autre part, elle prévoit la possibilité d'agréer des moyens d'identification électronique mobiles et non mobiles qui peuvent être utilisés pour accéder à des applications belges. À cette fin, la loi relative à l'identification électronique prévoit les dispositions nécessaires.

D. **COMMENTAIRE DES ARTICLES**

CHAPITRE 1ER

Disposition générale

Article 1er

Cet article ne requiert aucun commentaire particulier.

CHAPITRE 2

Définitions

Article 2

L'article 2, § 1er, 1° du présent projet prévoit que lorsqu'il est question de "règlement 910/2014", il s'agit du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE. En effet, vu que ce projet vise à la pleine mise en œuvre du chapitre II de ce règlement (identification électronique), il est utile de définir ce terme afin de rendre le texte plus lisible, quand il est fait référence à l'ensemble ou à une partie des dispositions du règlement. Il en va de même pour les règlements d'exécution du règlement 910/2014 auxquels il est fait référence.

L'article 2 § 1er, 4° du projet renvoit à l'article 6 pour le concept de l'organe de contrôle. Même si ce concept n'est pas utilisé dans le règlement 910/2014 dans le contexte du chapitre II (identification électronique),

volgt uit artikel 9, 1, b) van verordening 910/2014 de plicht voor lidstaten om een toezichtregeling te voorzien voor aangemelde stelsels voor elektronische identificatie. Om te voldoen aan deze verplichting inzake toezichtregeling voorziet dit ontwerp de aanduiding van een toezichthoudend orgaan.

Het toezichthoudend orgaan, zoals hier bedoeld, heeft geen enkele bevoegdheid om toezichthoudende taken uit te voeren die betrekking hebben op vertrouwensdiensten.

Artikel 2 § 1, 5° van dit ontwerp verwijst voor het begrip knooppunt naar de uitvoeringsverordening (EU) 2015/1501.

Paragraaf 2 van artikel 2 vereist geen bijzondere commentaar.

HOOFDSTUK 3

Grensoverschrijdende elektronische identificatie

Afdeling 1

Wederzijdse erkenning

Artikel 3

Lidstaten dienen de private sector aan te moedigen om vrijwillig gebruik te maken van elektronische identificatiemiddelen die onder een aangemeld stelsel vallen. De lidstaat mag overeenkomstig artikel 7, f), lid 2 van verordening 910/2014 echter voorwaarden stellen voor toegang tot die elektronische identificatie. Dit artikel belast de Koning met het vaststellen van de voorwaarden waaraan private instanties moeten voldoen om gebruik te maken van de door de overheid aangeboden online identificatie. Als er een impact is op het vlak van persoonsgegevens zal hierover uiteraard het advies gevraagd worden van de Commissie voor de bescherming van de persoonlijke levenssfeer.

Afdeling 2

Betrouwbaarheidsniveaus

Artikel 4

Om aan de verplichting tot wederzijdse erkenning zoals bedoeld in artikel 6 van verordening 910/2014 te voldoen, moet elke overheidsdienst bepalen welk betrouwbaarheidsniveau nodig is om toegang te krijgen tot haar diensten. Binnen dat niveau en de hogere

l'obligation pour les États membres de prévoir un régime de contrôle pour les schémas d'identification électronique notifiés découle de l'article 9, 1, b) du règlement 910/2014. Pour satisfaire à cette obligation relative au régime de contrôle, le présent projet prévoit la désignation d'un organe de contrôle.

L'organe de contrôle dont question n'a cependant aucune compétence pour exécuter des tâches de contrôle relatives aux services de confiance.

L'article 2 § 1er, 5° du présent projet fait référence au règlement (UE) 2015/1501 pour le concept de nœud.

Le paragraphe 2 de l'article 2 ne requiert aucun commentaire particulier.

CHAPITRE 3

Identification électronique transfrontalière

Section 1re

Reconnaissance mutuelle

Article 3

Les États membres doivent encourager le secteur privé à utiliser volontairement des moyens d'identification électronique relevant d'un schéma notifié. Conformément à l'article 7, f), alinéa 2 du règlement 910/2014, l'État membre peut cependant définir les conditions d'accès à cette identification électronique. Cet article charge le Roi de fixer les conditions auxquelles des instances privées doivent satisfaire pour pouvoir utiliser l'identification en ligne offerte par l'Administration. S'il existe un impact sur les données à caractère personnel, l'avis de la Commission de la protection de la vie privée sera bien entendu demandé.

Section 2

Niveaux de garantie

Article 4

Pour satisfaire à l'obligation de reconnaissance mutuelle telle que visée à l'article 6 du règlement 910/2014, chaque service public doit déterminer quel niveau de garantie est nécessaire pour accéder à ses services. Au sein de ce niveau et des niveaux plus élevés, le citoyen

niveaus heeft de burger de keuze tussen één of meer identificatiemiddelen om zich dan effectief toegang te verschaffen tot de overheidstoepassing.

Volgens verordening 910/2014 zal de overheidsdienst die binnen de Belgische context de niveaus "substantieel" en "hoog" toelaat ook de Europees aangemelde identificatiemiddelen uit andere lidstaten met een overeenstemmend of hoger betrouwbaarheidsniveau dienen toe te laten voor inwoners van andere Europese lidstaten. Of de persoon al dan niet werkelijk toegang krijgt tot de dienst wordt door de overheidsdienst bepaald.

Deze verplichting is niet voorzien in de verordening 910/2014 maar is wel nodig om te weten welke aangemelde identificatiemiddelen moeten worden aanvaard door de overheidsdiensten. Deze verplichting vloeit ook niet voort uit de aanduiding van een uniek loket want de samenwerking die via het uniek loket wordt opgelegd betreft een samenwerking tussen de lidstaten en geen informatieverplichting binnen een lidstaat.

Daarnaast moeten de betrouwbaarheidsniveaus voor de bij de Commissie aan te melden elektronische identificatiemiddelen bepaald worden in overeenstemming met Uitvoeringsverordening (EU) 2015/1502. Paragraaf 2 van dit artikel legt de bevoegdheid hiervoor bij de instantie aangeduid door de Koning. Bij de bepaling van het betrouwbaarheidsniveau is het nodig om de impact van de bepaling van het betrouwbaarheidsniveau op de gebruikers te evalueren.

De hierboven vermelde instantie zorgt in naam van de Belgische overheid voor aanmelding bij de Europese Commissie van één of meerdere Belgische stelsels voor elektronische identificatie overeenkomstig artikel 9 van verordening 910/2014. De bepaling delegeert aan de Koning de aanduiding van een instantie om deze aanmelding concreet vorm te geven.

Afdeling 3

Persoonsidentificatiegegevens en toegang tot het Rijksregister

Artikel 5

De uitvoeringsverordening (EU) 2015/1501 bevat bepalingen in verband met de uitwisseling en de beveiliging van informatie die dient te worden uitgewisseld tussen de lidstaten in het kader van grensoverschrijdende identificatie.

Zo is er een minimale set persoonsidentificatiegegevens gedefinieerd in artikel 11 en in de bijlage

a le choix entre un ou plusieurs moyens d'identification pour accéder effectivement à l'application publique.

Selon le règlement 910/2014, le service public qui, dans le contexte belge, autorise les niveaux "substantiel" et "élevé", devra aussi autoriser pour les habitants d'autres États membres européens des moyens d'identification européens notifiés d'autres États membres disposant d'un niveau de garantie correspondant ou supérieur. Le fait que la personne accède effectivement ou non au service est déterminé par le service public.

Cette obligation n'est pas prévue dans le règlement 910/2014 mais est cependant nécessaire pour savoir quels moyens d'identification notifiés doivent être acceptés par les services publics. Cette obligation ne découle pas non plus de la désignation d'un guichet unique étant donné que la collaboration imposée par le biais de ce guichet unique se fait entre les États membres et ne constitue pas une obligation d'information au sein d'un État membre.

Par ailleurs, les niveaux de garantie pour les moyens d'identification électronique à notifier à la Commission doivent être déterminés conformément au Règlement d'exécution (UE) 2015/1502. Le paragraphe 2 de cet article attribue la compétence en la matière à l'instance désignée par le Roi. Pour déterminer le niveau de garantie, il est nécessaire d'évaluer l'impact de la définition du niveau de garantie sur les utilisateurs.

L'instance susmentionnée se charge au nom de l'Administration belge de la notification à la Commission européenne d'un ou de plusieurs schémas d'identification électronique belges conformément à l'article 9 du règlement 910/2014. La disposition délègue au Roi la désignation d'une instance pour donner concrètement forme à cette notification.

Section 3

Données d'identification personnelle et accès au Registre national

Article 5

Le règlement d'exécution (UE) 2015/1501 prévoit des dispositions relatives à l'échange et à la sécurité des informations qui doivent être échangées entre les États membres dans le cadre de l'identification transfrontalière.

Ainsi, un ensemble minimum de données d'identification personnelle a été défini à l'article 11 et à l'annexe

van de hierboven vermelde uitvoeringsverordening. Deze informatie zal worden uitgewisseld wanneer een persoon die houder is van een Belgisch elektronische identificatiemiddel, zich wenst toegang te verschaffen tot online toepassingen in het buitenland. Uiteraard zal de gebruiker hierover geïnformeerd worden.

Dit artikel geeft aan de instantie aangeduid door de Koning de opdracht om voor het uitwisselen van deze informatie het Rijksregister te consulteren. Conform het advies nr 48/2016 van de Commissie voor de bescherming van de persoonlijke levenssfeer, zal bij uitwisseling van gegevens in toepassing van artikel 7, f), tweede lid van de verordening 910/2014 aan niet openbare instanties slechts een beperkt pakket persoonsidentificatiegegevens worden meegestuurd.

Bij nieuwe toekomstige bepalingen die voorzien om facultatieve persoonsidentificatigegevens uit te wisselen conform verordening 910/2014 of één van haar uitvoeringshandelingen, zal eveneens het Rijksregister worden geconsulteerd, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer.

Afdeling 4

Toezicht en controle

Artikel 6

Overeenkomstig artikel 9, lid 1, b) van verordening 910/2014 geeft de aanmeldende lidstaat de Commissie onverwijld kennis van de toepasselijke toezichtregeling en informatie over de aansprakelijkheidsregeling met betrekking tot de partij die het elektronische identificatiemiddel uitgeeft en de partij die de authenticatieprocedure uitvoert.

Overeenkomstig artikel 9, lid 1, g) van verordening 910/2014 geeft de aanmeldende lidstaat ook onverwijld kennis van de regeling voor de opschorting of intrekking van het aangemelde stelsel voor elektronische identificatie of de delen waarvan de integriteit is geschonden.

Een dergelijke regeling ontbreekt vandaag in België. Teneinde te kunnen voldoen aan bovenstaande door verordening 910/2014 gestelde informatieverplichtingen, bepaalt artikel 6 van dit ontwerp dat een toezichtsorgaan wordt opgericht, bestaande uit vertegenwoordigers van 3 verschillende overheidsdiensten die een expertise hebben in het domein van elektronische identificatie. Het toezicht zal onder andere bestaan uit preventie, monitoring en controle.

du règlement d'exécution susmentionné. Ces informations seront échangées lorsqu'une personne titulaire d'un moyen d'identification électronique belge souhaitera accéder à des applications en ligne à l'étranger. L'utilisateur en sera bien entendu informé.

Le présent article confère à l'instance désignée par le Roi la mission de consulter le Registre national pour échanger ces informations. Conformément à l'avis n° 48/2016 de la Commission de la protection de la vie privée, l'échange de données, en application de l'article 7, f), deuxième alinéa du règlement 910/2014, avec des instances non publiques n'entraînera la transmission que d'un ensemble minimal de données d'identification personnelle.

En cas de nouvelles dispositions futures qui prévoient l'échange de données d'identification personnelle facultatives conformément au règlement 910/2014 ou à l'un de ses actes d'exécution, le Registre national sera également consulté, après avis de la Commission de la protection de la vie privée.

Section 4

Surveillance et contrôle

Article 6

Conformément à l'article 9, alinéa 1er, b) du règlement 910/2014, l'État membre notifiant notifie dans les meilleurs délais à la Commission le régime de contrôle applicable et des informations sur la responsabilité en ce qui concerne la partie qui délivre le moyen d'identification électronique et la partie qui gère la procédure d'authentification.

Conformément à l'article 9, alinéa 1er, g) du règlement 910/2014, l'État membre notifiant notifie également dans les meilleurs délais les dispositions concernant la suspension ou la révocation du schéma d'identification électronique notifié ou des parties compromises concernées.

Un tel règlement fait actuellement défaut en Belgique. Afin de pouvoir répondre aux obligations d'information précitées du règlement 910/2014, l'article 6 du présent projet précise qu'un organe de contrôle sera créé et sera composé de représentants de 3 services publics différents disposant d'une expertise dans le domaine de l'identification électronique. Le contrôle consistera notamment en de la prévention, de la surveillance et de la vérification.

De Verordening voorziet geen orgaan voor het toezicht op de aangemelde schema's voor elektronische identificatie. Het lijkt echter raadzaam dat deze bevoegdheid van toezicht wordt toegewezen aan een orgaan in plaats van *ad hoc* te bekijken wat de toezichtregeling is.

Wanneer aangewezen kan het toezichthoudend orgaan zich laten bijstaan door deskundigen.

Het toezichthoudend orgaan kan in gebreke blijvende partijen verzoeken om de nodige maatregelen te treffen om tekortkomingen te verhelpen en de dienstverlening te verbeteren of vragen om een externe audit. Deze maatregelen ter verbetering kunnen enkel opgelegd worden bij inbreuken waarbij de persoonsgegevens niet in gevaar komen (verlies, ongeoorloofde wijziging, ongeoorloofde toegang, diefstal) want bij inbreuken waarbij de persoonsgegevens in gevaar komen volgt onmiddellijk opschorting of intrekking.

Wanneer de integriteit van een aangemeld stelsel in het gedrang is, zullen de ministers verantwoordelijk voor de aangemelde stelsels voor elektronische identificatie op advies van het toezichthoudend orgaan het stelsel geheel of gedeeltelijk intrekken of opschorten, en de Europese Commissie en de lidstaten verwittigen. In het geval er een integriteitsprobleem is, moet onmiddellijk worden ingegrepen om identiteitsfraude, ongeoorloorde toegang en gebruik van persoonsgegevens of andere zware problemen te voorkomen.

Het toezichthoudend orgaan zal jaarlijks rapporteren aan de bevoegde ministers.

Hoewel de Raad van State in haar advies verwijst naar artikel 16 Verordening 910/2014 – dat bepaalt dat de lidstaten de voorschriften vaststellen inzake de sancties die van toepassing zijn op inbreuken op de verordening – heeft het artikel geen betrekking op elektronische identificatie. Artikel 16 Verordening 910/2014 is namelijk van toepassing op de vertrouwensdiensten. In België werd op basis van dit artikel reeds voorzien in een sanctiemechanisme in het Wetboek Economisch Recht.

Afdeling 5

Samenwerking en interoperabiliteit

Artikel 7

Overeenkomstig artikel 3 van het Uitvoeringsbesluit 2015/296 van 24 februari 2015 van de Commissie tot vaststelling van procedurele voorschriften betreffende de samenwerking tussen de lidstaten op het gebied van elektronische identificatie overeenkomstig artikel

Le Règlement ne prévoit pas d'organe pour le contrôle des schémas d'identification électronique notifiés. Il semble néanmoins indiqué d'attribuer cette compétence de contrôle à un organe plutôt que d'examiner *ad hoc* la réglementation relative au contrôle.

Lorsque c'est indiqué, l'organe de contrôle peut se faire assister par des experts.

L'organe de contrôle peut mettre en demeure les parties défaillantes et les inviter à prendre les mesures nécessaires pour combler des défaillances et améliorer la prestation de services ou demander un audit externe. Ces mesures d'amélioration ne peuvent être imposées qu'en cas d'infractions ne causant pas de préjudice aux données à caractère personnel (perte, modification illicite, accès illicite, vol). En effet, tout préjudice à des données à caractère personnel entraîne immédiatement une suspension ou une révocation.

Lorsque l'intégrité d'un schéma notifié est menacée, les ministres responsables des schémas d'identification électronique notifiés, sur conseil de l'organe de contrôle, révoqueront ou suspendront une partie ou la totalité du schéma et en avertiront la Commission européenne ainsi que les États membres. En cas de problème d'intégrité, il convient d'intervenir immédiatement afin de prévenir la fraude à l'identité, un accès illicite et l'utilisation de données à caractère personnel, ou toute autre problème majeur.

L'organe de contrôle fera annuellement rapport aux ministres compétents.

Bien que, dans son avis, le Conseil d'État fasse référence à l'article 16 du Règlement 910/2014, qui précise que les États membres fixent le régime des sanctions applicables aux violations du règlement, l'article ne concerne pas l'identification électronique. L'article 16 du Règlement 910/2014 s'applique en effet aux services de confiance. En Belgique, un mécanisme de sanctions a déjà été prévu sur la base de cet article dans le Code de droit économique.

Section 5

Collaboration et interopérabilité

Article 7

Conformément à l'article 3 de la Décision d'exécution 2015/296 de la Commission du 24 février 2015 établissant les modalités de coopération entre les États membres en matière d'identification électronique conformément à l'article 12, paragraphe 7, du règlement

12, lid 7, van verordening 910/2014, moet de Belgische overheid, teneinde de samenwerking met de andere Europese lidstaten tot stand te brengen, één loket aanwijzen.

Artikel 7 van dit ontwerp bepaalt dat de Koning de instantie aanduidt die fungeert als één loket. De facto vervult de Federale overheidsdienst Beleid en Ondersteuning deze rol al.

Artikel 8

Overeenkomstig artikel 2 van Uitvoeringsverordening 2015/1501 heeft de exploitant van een knooppunt de taak om ervoor te zorgen dat het knooppunt correct en betrouwbaar als aansluitpunt functioneert.

Een knooppunt is een aansluitpunt dat onderdeel is van de interoperabiliteitsarchitectuur voor elektronische identificatie en betrokken is bij de grensoverschrijdende authenticatie van personen, en dat in staat is berichten te herkennen en te verwerken of door te sturen naar andere knooppunten door mogelijk te maken dat de nationale elektronische identificatie-infrastructuur van een lidstaat gekoppeld wordt aan de nationale elektronische identificatie-infrastructuren van andere lidstaten.

Conform de hierboven vermelde Uitvoeringsverordening dienen de knooppunten maatregelen te nemen in verband met de beveiliging van de gegevens.

Artikel 8 van dit ontwerp bepaalt dat de Koning de instantie aanduidt die fungeert als knooppuntexploitant. De facto vervult de Federale overheidsdienst Beleid en Ondersteuning deze rol al.

HOOFDSTUK 4

Elektronische identificatie voor Belgische overheidstoepassingen

Afdeling 1

Authenticatiedienst

Artikel 9

Binnen CSAM (een geheel van afspraken en van regels om het identiteits- en toegangsbeheer binnen het *e-government* te organiseren) baat de Federale overheidsdienst Beleid en Ondersteuning een authenticatiedienst ("*Federal Authentication Service*" of "FAS"), uit, als een essentiële bouwsteen voor e-government.

n° 910/2014, l'Administration belge doit désigner un guichet unique afin de mettre en place la coopération entre les États membres européens.

L'article 7 du présent projet prévoit que le Roi désigne l'instance qui fera office de guichet unique. De facto, le Service public fédéral Stratégie et Appui remplit déjà ce rôle.

Article 8

Conformément à l'article 2 du règlement d'exécution 2015/1501, l'exploitant d'un nœud doit faire en sorte que les fonctions du nœud en tant que point de connexion soient assurées de manière correcte et fiable.

Un nœud est un point de connexion qui fait partie de l'architecture de l'interopérabilité d'identification électronique et participe au processus d'authentification transfrontalière des personnes et qui a la capacité de reconnaître et de traiter ou d'envoyer des transmissions à d'autres nœuds en permettant à l'infrastructure d'identification électronique nationale d'un État membre de fonctionner en interface avec les infrastructures d'identification électronique nationales d'autres États membres.

Conformément au règlement d'exécution susmentionné, les nœuds doivent prendre des mesures relatives à la sécurisation des données.

L'article 8 du présent projet prévoit que le Roi désigne l'instance qui fera office d'exploitant du nœud. De facto, le Service public fédéral Stratégie et Appui remplit déjà ce rôle.

CHAPITRE 4

Identification électronique pour applications publiques belges

Section 1re

Service d'authentification

Article 9

Au sein de CSAM (un ensemble d'accords et de règles visant à organiser la gestion de l'identité et de l'accès au sein de l'e-gouvernement), le Service public fédéral Stratégie et Appui exploite un service d'authentification ("*Federal Authentication Service*" ou "FAS"), qui constitue un fondement essentiel de l'e-gouvernement.

Dit past binnen diens opdracht tot het ontwikkelen en beheren van digitale diensten en platformen met het oog op digitale interactie met burgers en ondernemingen en tussen administraties.

De FAS is een authenticatiedienst gebaseerd op verschillende elektronische identificatiemiddelen om burgers toegang te geven tot digitale overheidstoepassingen met verschillende beveiligingsniveaus die overeenkomstig verordening 910/2014 beoordeeld werden als laag, substantieel en hoog. Er is dus een gelijkstelling met de niveaus zoals die bestaan in de verordening 910/2014 zonder dat er per se enige aanmelding is conform verordening 910/2014. Een ondubbelzinnige wettelijke basis voor de uitbating van de authenticatiedienst ontbreekt tot op heden. Om die reden voorziet artikel 9 van dit ontwerp in de nodige wettelijke verankering van de federale authenticatiedienst, waarbij ook in de verplichting wordt voorzien om te zorgen voor de beschikbaarheid van de federale authenticatiedienst.

Wanneer de Federale overheidsdienst Beleid en Ondersteuning dat nodig acht kan zij voor de exploitatie van de authenticatiedienst samenwerken met andere overheidsdiensten en/of met private partners.

De Federale overheidsdienst Beleid en Ondersteuning wordt bij wet aangeduid met het oog op het vrijwaren van de rechten van de burger. De tekst bevat immers regels die ruimer zijn dan enkel het organiseren van een dienst van de uitvoerende macht en hebben een impact op andere partijen dan de Belgische Staat zelf. De authenticatiedienst is een dienst die de authenticatie doet van burgers wanneer ze toegang wensen tot overheidstoepassingen en heeft dus een rechtstreekse impact op hen en op de bescherming van hun persoonlijke levenssfeer. Het rijksregisternummer van de burgers wordt gebruikt als ook andere persoonsgegevens.

Overeenkomstig de beraadslaging RR 21/2015 van het sectoraal comité van het Rijksregister heeft de Federale overheidsdienst Beleid en Ondersteuning als rechtsopvolger van de Federale overheidsdienst Informatie- en Communicatietechnologie het recht om het rijksregisternummer te gebruiken bij aanwending van de federale authenticatiedienst voor toegangs- en gebruikersbeheer voor informatietoepassingen voor opdrachten van algemeen belang. Het gebruik van het rijksregisternummer is noodzakelijk om de identificatie en de authenticatie van personen correct te laten verlopen. Het gaat om een uniek nummer waarmee een persoon met grote nauwkeurigheid kan worden geïdentificeerd. De federale authenticatiedienst kan zo bijdragen aan het respecteren door de federale instanties van de verplichting in artikel 4 § 1 van de wet van 5 mei 2014 houdende verankering van het principe van

Cette exploitation s'inscrit dans le cadre du développement et de la gestion des services numériques et des plateformes qui permettent l'interaction numérique avec les citoyens et les entreprises et entre administrations.

Le FAS est un service d'authentification basé sur différents moyens d'identification électronique permettant aux citoyens d'accéder à des applications publiques numériques assortis de différents niveaux de sécurité qui, conformément au règlement 910/2014, ont été qualifiés de faibles, substantiels et élevés. Il y a donc une équivalence avec les niveaux définis dans le règlement 910/2014 sans qu'aucune notification ne soit faite conformément au règlement 910/2014. Il n'existe actuellement aucune base légale explicite pour l'exploitation du service d'authentification. C'est la raison pour laquelle l'article 9 du présent projet prévoit l'ancrage légale nécessaire du service fédéral d'authentification, ainsi que l'obligation de veiller à la disponibilité du service fédéral d'authentification.

Lorsque le Service public fédéral Stratégie et Appui l'estime nécessaire, il peut, pour l'exploitation du service d'authentification, collaborer avec d'autres services publics fédéraux et/ou avec des partenaires privés.

Le Service public fédéral Stratégie et Appui est désigné légalement afin de garantir les droits des citoyens. En effet, le texte contient des règles qui vont au-delà de la seule organisation d'un service du pouvoir exécutif et qui ont un impact sur des parties autres que l'État belge lui-même. Le service d'authentification est un service qui authentifie les citoyens qui souhaitent accéder à des applications publiques. Il a donc un impact direct sur les citoyens et sur la protection de leur vie privée. Le numéro de Registre national des citoyens, ainsi que d'autres données à caractère personnel, sont utilisés.

Conformément à la Délibération RN n° 21/2015 du Comité sectoriel du Registre national, le Service public fédéral Stratégie et Appui, en tant que successeur légal du Service public fédéral Technologie de l'Information et la Communication, a le droit d'utiliser le numéro de Registre national dans le cadre du recours au service fédéral d'authentification pour la gestion des accès et des utilisateurs aux applications informatiques développées dans le cadre de missions de service public. L'utilisation du numéro de Registre national est nécessaire pour procéder correctement à l'identification et à l'authentification de personnes. Il s'agit d'un numéro unique permettant d'identifier une personne avec une grande précision. Le service fédéral d'authentification peut ainsi contribuer au respect par les instances fédérales de l'obligation prévue à l'article 4, 1er, de la loi du 5 mai 2014 garantissant le principe de la collecte unique

de unieke gegevensinzameling in de werking van de diensten en instanties die behoren tot of taken uitvoeren voor de overheid en tot vereenvoudiging en gelijkschakeling van elektronische en papieren formulieren. Deze bepaling verplicht federale instanties om bij de uitvoering van hun opdrachten het rijksregisternummer te gebruiken voor de identificatie van natuurlijke personen.

Afdeling 2

Erkenning elektronische identificatiemiddelen

Artikel 10

Momenteel kunnen burgers voor digitale overheidstoepassingen (bijvoorbeeld *Tax-on-web*) gebruik maken van verschillende inlogmogelijkheden (verzameld en gezamenlijk aangeboden binnen de FAS), waaronder de elektronische identificatie op basis van de elektronische identiteitskaart. De elektronische identiteitskaart bevat een handtekeningscertificaat om elektronische handtekeningen te plaatsen en een identiteitscertificaat waarmee men online zijn identiteit kan bewijzen.

Op basis van het identiteitscertificaat kunnen de burgers toegang krijgen tot overheidstoepassingen, niet zelden tot hun eigen gegevens waarover de overheid beschikt.

Op dit moment heeft de burger voor online inloggen met de elektronische identiteitskaart meestal een verbonden kaartlezer nodig en onderzoek wijst uit dat niet iedereen over zo'n kaartlezer beschikt. Bovendien moet men voor het gebruik van de kaartlezer eID-software installeren. Het is een eenvoudige handeling maar bouwt toch een drempel in voor het gebruik.

In een snel evoluerende digitale wereld waar de burger op verschillende manieren en vanop verschillende toestellen, met inbegrip van mobiele toestellen zoals tablets en smartphones, in contact wenst te treden met de overheid, staat de overheid voor de uitdaging het groeiend aanbod van digitale overheidstoepassingen eveneens open te stellen voor deze nieuwe mobiele toestellen.

De overheid wenst met dit ontwerp de identificatiemogelijkheden binnen de authenticatiedienst voor digitale overheidstoepassingen uit te breiden en het gebruik van mobiel en niet mobiele identificatie eenvoudiger te maken voor burgers. Een erkenning in België voor opname in de Belgische authenticatiedienst staat los van een

des données dans le fonctionnement des services et instances qui relèvent de ou exécutent certaines missions pour l'autorité et portant simplification et harmonisation des formulaires électroniques et papier. Cette disposition oblige les instances fédérales à utiliser, dans le cadre de l'exécution de leurs missions, le numéro de Registre national pour l'identification des personnes physiques.

Section 2

Reconnaissance des moyens d'identification électronique

Article 10

Pour accéder à des applications publiques numériques (par exemple *Tax-on-web*), les citoyens disposent actuellement de différentes possibilités d'identification (toutes rassemblées et offertes au sein du FAS), parmi lesquelles l'identification électronique sur la base de la carte d'identité électronique. La carte d'identité électronique contient un certificat de signature permettant d'apposer des signatures électroniques et un certificat d'identité permettant de prouver l'identité en ligne.

Sur la base du certificat d'identité, les citoyens peuvent accéder à des applications publiques et il n'est pas rare qu'ils puissent consulter leurs propres données dont l'Administration dispose.

Actuellement, le citoyen qui désire s'identifier en ligne à l'aide de sa carte d'identité électronique a généralement besoin d'un lecteur de cartes filaire. Une enquête montre cependant que tout le monde ne dispose pas d'un tel lecteur de cartes. De plus, l'utilisation du lecteur de cartes nécessite l'installation du logiciel eID. Il s'agit d'une opération simple mais qui représente tout de même un obstacle.

Dans un monde numérique en évolution rapide dans lequel le citoyen souhaite entrer en contact avec l'Administration de différentes manières et à partir de plusieurs appareils, y compris des appareils mobiles comme des tablettes et des smartphones, l'Administration doit relever le défi consistant à ouvrir à ces nouveaux appareils mobiles l'offre croissante d'applications publiques numériques.

Par le biais du présent projet, l'Administration souhaite étendre les possibilités d'identification au sein du service d'authentification pour les applications publiques numériques et simplifier l'utilisation des identifications mobiles et non mobiles pour les citoyens. Une reconnaissance en Belgique à des fins d'intégration

aanmelding bij de Europese Commissie overeenkomstig verordening 910/2014. Sommige identificatiemiddelen zullen niet aangemeld worden overeenkomstig de verordening 910/2014 maar enkel gebruikt worden binnen de Belgische context.

Artikel 10 van dit ontwerp strekt er in het bijzonder toe een kader te scheppen waarbinnen de Federale overheidsdienst Beleid en Ondersteuning, na consultatie van vertegenwoordigers van het College van voorzitters van de federale en programmatorische overheidsdiensten, van het College van afgevaardigd bestuurders van de instellingen van sociale zekerheid en van het College van afgevaardigd bestuurders van de federale instellingen van openbaar nut, diensten voor elektronische identificatie, al dan niet gebaseerd op mobiele middelen voor elektronische identificatie, kan erkennen zodat deze erkende diensten burgers toegang mogen geven via de authenticatiedienst tot digitale overheidstoepassingen in België.

Het doel van een erkenning is dus dat de erkende diensten voor elektronische identificatie, al dan niet betalend, worden opgenomen als één van de inlogmogelijkheden voor Belgische digitale overheidstoepassingen op het toegangsportaal van de authenticatiedienst.

De Federale overheidsdienst Beleid en Ondersteuning wordt bij wet aangeduid met het oog op het vrijwaren van de rechten van de burgers en ondernemingen. De tekst bevat immers regels die ruimer zijn dan enkel het organiseren van een dienst van de uitvoerende macht en hebben een impact op andere partijen dan de Belgische staat zelf (burgers, ondernemingen). De regels voorzien dat ondernemingen erkend kunnen worden door de Federale overheidsdienst Beleid en Ondersteuning om ook hun diensten aan te bieden voor toegang van burgers tot overheidstoepassingen. Er worden dus een aantal voorwaarden voor ondernemingen voorzien. De authenticatiedienst is een dienst die de authenticatie doet van burgers wanneer ze toegang wensen tot overheidstoepassingen en heeft dus ook een rechtstreekse impact op hen en op de bescherming van hun persoonlijke levenssfeer.

Het is voor de erkenning niet noodzakelijk dat één partij de hele dienst voor elektronische identificatie aanbiedt. Eén partij kan bijvoorbeeld de inschrijving (registratie en verificatie van de identiteit) doen, een andere de rest van de dienst aanbieden. Om als één van de inlogmogelijkheden te worden opgenomen conform deze regeling is het wel nodig dat heel de dienst voor elektronische identificatie erkend is.

dans le service d'authentification belge est indépendante de la notification à la Commission Européenne conformément au règlement 910/2014. Certains moyens d'identification ne seront pas notifiés conformément au règlement 910/2014 mais uniquement utilisés dans le contexte belge.

L'article 10 du présent projet vise en particulier à créer un cadre dans lequel le Service public fédéral Stratégie et Appui désigne une instance qui, après consultation de représentants du Collège des présidents des service publics fédéraux et des services publics de programmation, du Collège des administrateurs délégués des institutions de la sécurité sociale et du Collège des administrateurs délégués des organismes d'intérêt public fédéraux, peut agréer des services d'identification électronique basés ou non sur des moyens d'identification électronique mobiles afin que ces services agréés puissent permettre aux citoyens d'accéder via le service d'authentification aux applications publiques numériques en Belgique.

L'agrément a donc pour objectif que les services d'identification électronique agréés, payants ou non, soient repris comme faisant partie des possibilités d'identification pour des applications publiques numériques belges sur le portail d'accès du service d'authentification.

Le Service public fédéral Stratégie et Appui est désigné légalement afin de garantir les droits des citoyens et des entreprises. En effet, le texte contient des règles qui vont au-delà de la seule organisation d'un service du pouvoir exécutif et qui ont un impact sur des parties autres que l'État belge lui-même (citoyens, entreprises). Les règles prévoient que les entreprises peuvent être agréées par le Service public fédéral Stratégie et Appui pour offrir également aux citoyens leurs services d'accès à des applications publiques. Une série de conditions sont donc prévues pour les entreprises. Le service d'authentification est un service qui authentifie les citoyens qui souhaitent accéder à des applications publiques. Il a donc également un impact direct sur les citoyens et sur la protection de leur vie privée.

Pour l'agrément, il n'est pas nécessaire qu'une seule partie offre l'ensemble du service d'identification électronique. Une partie peut par exemple procéder à l'enregistrement (enregistrement et vérification de l'identité) et une autre offrir le reste du service. Cependant, pour être considéré comme l'une des possibilités d'identification conformément à la présente réglementation, le service d'identification électronique doit être agréé dans son ensemble.

De door de Koning vast te stellen voorwaarden voor erkenning dienen minstens betrekking te hebben op functionele en technische kenmerken, op respect voor de persoonlijke levenssfeer en invulling van veiligheidsvereisten, op dienstverleningsbeheer en op juridische en economische kenmerken.

Er zullen garanties gevraagd worden om te beletten dat gegevens voor andere doeleinden dan identificatie en authenticatie kunnen worden gebruikt.

De voorwaarden dienen te worden voorgelegd aan de Commissie voor de bescherming van de persoonlijke levenssfeer.

Het geheel van voorwaarden dient gepubliceerd te worden op de website van de authenticatiedienst.

De Federale overheidsdienst Beleid en Ondersteuning kan zich voor de erkenning laten bijstaan door experten indien nodig. Gespecialiseerde experten kunnen bijvoorbeeld ingezet worden om veiligheidsaspecten te checken.

Na erkenning kunnen ook private spelers elektronische identificatiemiddelen voor toegang tot digitale overheidstoepassingen aanbieden onafhankelijk van de overheid maar erkend door de overheid.

Eén van de operationele gevolgen van de erkenning is dat de aanbieder van de erkende aanmeldingsdienst wordt beschouwd als een onderaannemer van de erkennende overheid in de zin van artikel 5, eerste lid, 3°, van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen. De onderaannemer van de erkennende overheid is dan in die hoedanigheid gemachtigd om het rijksregisternummer te gebruiken enkel voor het toegangs- en gebruikersbeheer voor overheidstoepassingen via de *Federal Authentication Service* (FAS). Het gebruik van het rijksregisternummer is dus beperkt tot het uitvoeren van de opdrachten van identificatie en authenticatie voor de federale authenticatiedienst. Voor gebruik van het rijksregisternummer buiten de erkenning dient uiteraard een aparte machtiging te worden bekomen.

De Federale overheidsdienst Beleid en Ondersteuning kan controles uitvoeren om te verifiëren of een erkende dienst aan de voorwaarden voldoet en desgevallend de nodige maatregelen nemen indien dat niet het geval is. Deze maatregelen kunnen bestaan uit het opleggen van maatregelen ter verbetering van de dienstverlening, intrekking of schorsing.

Les conditions d'agrément à fixer par le Roi doivent au moins concerner les caractéristiques fonctionnelles et techniques, le respect de la vie privée et d'exigences de sécurité, la gestion des services ainsi que les caractéristiques juridiques et économiques.

Des garanties seront demandées afin d'empêcher que des données ne soient utilisées à des fins autres que l'identification et l'authentification.

Les conditions doivent être soumises à la Commission de la protection de la vie privée.

L'ensemble des conditions doit être publié sur le site web du service d'authentification.

Le Service public fédéral Stratégie et Appui peut, si nécessaire, se faire assister par des experts pour l'agrément. Des experts spécialisés peuvent par exemple être engagés pour vérifier des aspects relatifs à la sécurité.

Après l'agrément, des acteurs privés également peuvent offrir des moyens d'identification électronique indépendants de l'Administration mais reconnus par celle-ci, pour accéder à des applications publiques numériques.

L'une des conséquences opérationnelles de l'agrément est que le fournisseur du service d'identification agréé est considéré comme sous-traitant de l'autorité d'agrément au sens de l'article 5, alinéa 1er, 3°, de la loi du 8 août 1983 organisant un Registre national des personnes physiques. En cette qualité, le sous-traitant de l'autorité d'agrément est dès lors autorisé à utiliser le numéro de Registre national uniquement pour la gestion de l'accès et des utilisateurs sur des applications publiques par le biais du service fédéral d'authentification (FAS). L'utilisation du numéro de Registre national est donc limitée à l'exécution des missions d'identification et authentification pour le service fédéral d'authentification. Pour l'utilisation du numéro de Registre national ne relevant pas de l'agrément, il va de soi qu'une autorisation distincte doit être obtenue.

Le Service public fédéral Stratégie et Appui peut procéder à des contrôles afin de vérifier si un service agréé répond aux conditions et prendre le cas échéant les mesures nécessaires si ces conditions ne sont pas respectées. Ces mesures peuvent comprendre l'imposition de mesures d'amélioration de la prestation de services, de révocation ou de suspension.

Een eventuele vergoedingsregeling voor betaling van erkende diensten voor elektronische identificatie door de erkennende overheid wordt vastgesteld door de Koning.

Zo'n vergoedingsregeling moet zich beperken tot een minimale onkostenvergoeding en houdt rekening met het feit dat een erkende aanbieder al een zekere mate van visibiliteit geniet door haar diensten te mogen aanbieden binnen de FAS.

Naar aanleiding van het advies 60 899/4 van 20 februari 2017 van de Raad van State werd de kwalificatie van de erkenningsregeling herbekeken. De erkenningsregeling kan noch gekwalificeerd worden als overheidsopdracht, noch als dienstenconcessie. De aanbieder van de dienst voor elektronische identificatie ontvangt namelijk geen tegenprestatie voor de diensten die hij aanbiedt, noch van de erkennende overheid, noch van de gebruikers. Hij ontvangt louter een onkostenvergoeding. De vergoeding is enkel bedoeld ter dekking van een deel van de kosten om verbinding te maken met de authenticatiedienst.

Het systeem van erkenning is er op gericht om een flexibele oplossing aan te bieden waarbij de overheid – d.m.v. erkenningsvoorwaarden – vat blijft houden op de kwalitatieve vereisten van zowel de dienstverlener als de dienst zelf.

Bovendien is de erkenningsregeling conform de bepalingen in de Richtlijn 2006/123/EG van het Europees Parlement en de Raad van 12 december 2006 betreffende diensten op de interne markt, hierna "Dienstenrichtlijn" genoemd. De erkenningsregeling kan vooreerst niet worden beschouwd als een vergunningsregeling in de zin van de Dienstenrichtlijn. In tegenstelling tot een systeem van vergunningen, betreft het geen stelsel dat individuele uitzonderingen verleent op een vooraf bepaalde verbodsregel. Er wordt derhalve geen verbod ingevoerd voor het aanbieden van gelijkaardige diensten. Daarnaast wordt een erkenningssysteem in beginsel gekenmerkt door het *intuitu personae* karakter ervan. De erkende dienstverlener krijgt deze erkenning namelijk omdat hijzelf voldoet aan de door de overheid vastgestelde eisen. Een vergunning daarentegen wordt verleend op basis van de specifieke kenmerken van de dienst zelf.

Een erkenningssysteem houdt op zich dus geen belemmering in voor de toegang tot of de uitoefening van de diensten. Tot slot mag het uitvoeringsbesluit geen eisen bevatten die de toegang tot of de uitoefening van een dienst belemmeren. Er zullen integendeel garanties opgenomen worden om discriminatie te vermijden. De economische en juridische voorwaarden zullen zo

Un éventuel régime d'indemnités relatif au paiement, par l'autorité d'agrément, des services d'identification électronique agréés est fixé par le Roi.

Un tel régime d'indemnités doit se limiter à un remboursement minimal des frais et tient compte du fait qu'un fournisseur agréé bénéficie déjà d'une certaine mesure de visibilité en étant autorisé à offrir ses services au sein du FAS.

À la suite de l'avis 60 899/4 du 20 février 2017 du Conseil d'État, la qualification du régime d'agrément a été réexaminée. Le régime d'agrément ne peut être qualifié ni de marché public ni de concession de services. Le fournisseur du service d'identification électronique ne bénéficie en effet d'aucune contrepartie pour les services qu'il offre, ni de l'autorité d'agrément, ni des utilisateurs. Il ne reçoit qu'un remboursement des frais. Ce remboursement ne sert qu'à couvrir une partie des frais de connexion au service d'authentification.

Le système d'agrément vise à offrir une solution flexible permettant à l'Administration, au moyen de conditions d'agrément, de garder une prise sur les exigences qualitatives tant du prestataire de services que du service lui-même.

En outre, le régime d'agrément est conforme aux dispositions de la Directive 2006/123/CE du Parlement européen et du Conseil du 12 décembre 2006 relative aux services dans le marché intérieur, ci-après dénommée "Directive Services". Premièrement, le régime d'agrément ne peut pas être considéré comme un régime d'autorisation au sens de la Directive Services. Contrairement à un système d'autorisations, il ne s'agit pas d'un système permettant des exceptions individuelles à une règle d'interdiction prédéfinie. Il n'est dès lors pas interdit d'offrir des services similaires. Par ailleurs, un système d'agrément est en principe caractérisé par son caractère *intuitu personae*. Le prestataire de services agréé reçoit cet agrément parce qu'il répond aux exigences posées par l'Administration. En revanche, une autorisation est octroyée sur la base des caractéristiques spécifiques du service lui-même.

Un système d'agrément ne comprend donc en soi aucune entrave à l'accès aux services ou à l'exercice des services. Enfin, l'arrêté d'exécution ne peut pas comporter d'exigences entravant l'accès à un service ou l'exercice d'un service. Au contraire, des garanties seront prévues pour éviter la discrimination. Les conditions économiques et juridiques seront décrites le plus

objectief mogelijk beschreven worden, teneinde de gelijke behandeling van de aanbieders van diensten te garanderen.

Afdeling 3

Verplichtingen verbonden aan het elektronisch identificatiemiddel

Artikel 11

In dit artikel wordt gepreciseerd dat de burger die in het bezit is van een elektronisch identificatiemiddel een aantal verplichtingen heeft ter bescherming van zijn elektronische identificatiemiddel. Hij moet zorgen dat hij het middel onder zijn exclusieve controle houdt wat onder meer inhoudt dat paswoorden strikt confidentieel moeten worden gehouden. Hij moet alle nodige maatregelen nemen om diefstal, verlies of verspreiding van zijn elektronisch identificatiemiddel te voorkomen en om ingeval van diefstal, verlies of verspreiding zijn elektronisch identificatiemiddel onmiddellijk te laten intrekken.

Wanneer het elektronisch identificatiemiddel niet meer geldig is of ingetrokken is, mag de houder het niet meer wetens en willens gebruiken.

HOOFDSTUK 5

Inwerkingtreding

Artikel 12

Artikel 12 van dit ontwerp bepaalt dat de Koning de inwerkingtreding van hoofdstuk 3 zal vastleggen.

Hoofdstuk 3 van dit ontwerp dient in werking te treden vooraleer de overheid een stelsel voor elektronische identificatie aanmeldt bij de Commissie. Op 29 september 2018 treedt de verplichting voor lidstaten tot wederzijdse erkenning van elektronische identificatiemiddelen in werking waardoor het sterk aangewezen is om voor die datum hoofdstuk 3 van dit ontwerp in werking te laten treden

De inwerkingtreding van hoofdstuk 4 van dit ontwerp is niet onderhevig aan externe factoren en kan reeds plaatsvinden.

De vice-eersteminister en minister van Ontwikkelingssamenwerking, Digitale Agenda, Telecommunicatie en Post,

Alexander DE CROO

objectivement possible, afin de garantir le traitement égalitaire des fournisseurs de services.

Section 3

Obligations liées au moyen d'identification électronique

Article 11

Cet article précise que le citoyen en possession d'un moyen d'identification électronique a une série d'obligations visant à protéger son moyen d'identification électronique. Il doit garder le moyen sous son contrôle exclusif, ce qui implique entre autres que les mots de passe doivent être tenus strictement confidentiels. Il doit prendre toutes les mesures nécessaires pour éviter le vol, la perte ou la divulgation de son moyen d'identification électronique et pour le révoquer immédiatement en cas de vol, de perte ou de divulgation.

Lorsque le moyen d'identification électronique n'est plus valable ou est révoqué, le titulaire ne peut plus l'utiliser sciemment.

CHAPITRE 5

Entrée en vigueur

Article 12

L'article 12 du présent projet précise que le Roi détermine l'entrée en vigueur du chapitre 3.

Le chapitre 3 de ce projet doit entrer en vigueur avant que l'Administration ne notifie un schéma d'identification électronique à la Commission. Le 29 septembre 2018, l'obligation pour les États membres de reconnaissance mutuelle des moyens d'identification électronique entrera en vigueur. Il est dès lors fortement indiqué de faire entrer en vigueur avant cette date le chapitre 3 du présent projet.

L'entrée en vigueur du chapitre 4 du présent projet n'est pas soumise à des facteurs externes et peut déjà avoir lieu.

Le vice-premier ministre et ministre de la Coopération au développement, de l'Agenda numérique, des Télécommunications et de la Poste,

Alexander DE CROO

VOORONTWERP VAN WET

onderworpen aan het advies van de Raad van State

Voorontwerp van wet inzake elektronische identificatie

HOOFDSTUK 1

Algemene bepaling

Artikel 1

Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.

HOOFDSTUK 2

Definities en toepassingsgebied

Afdeling 1

Definities

Artikel 2

Deze wet voert enerzijds hoofdstuk II (elektronische identificatie) van verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG uit, en legt anderzijds bepaalde regels vast in verband met het juridisch kader voor elektronische identificatiemiddelen voor overheidstoepassingen in België.

Artikel 3

§ 1. Voor de toepassing van deze wet en de uitvoeringsbesluiten wordt verstaan onder:

1° verordening 910/2014: de verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG;

2° uitvoeringsverordening (EU) 2015/1501: de uitvoeringsverordening (EU) 2015/1501 van de Commissie van 8 september 2015 betreffende het interoperabiliteitskader bedoeld in artikel 12, lid 8, van verordening 910/2014

3° uitvoeringsverordening (EU) 2015/1502: de uitvoeringsverordening (EU) 2015/1502 van 8 september 2015 van de Commissie tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3 van verordening 910/2014;

AVANT-PROJET DE LOI

soumis à l'avis du Conseil d'État

Avant-projet de loi relatif à l'identification électronique

CHAPITRE 1ER

Disposition générale

Article 1er

La présente loi règle une matière visée à l'article 74 de la Constitution.

CHAPITRE 2

Définitions et champ d'application

Section 1re

Définitions

Article 2

La présente loi exécute d'une part le chapitre II (identification électronique) du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, et fixe d'autre part certaines règles liées au cadre juridique des moyens d'identification électronique sur des applications publiques en Belgique.

Article 3

§ 1er. Pour l'application de la présente loi et des arrêtés d'exécution, on entend par:

1° règlement 910/2014: le règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE;

2° règlement d'exécution (UE) 2015/1501: le règlement d'exécution (UE) 2015/1501 de la Commission du 8 septembre 2015 sur le cadre d'interopérabilité visé à l'article 12, paragraphe 8, du règlement 910/2014;

3° règlement d'exécution (UE) 2015/1502: le règlement d'exécution (UE) 2015/1502 de la Commission européenne du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3, du règlement 910/2014;

4° toezichthoudend orgaan: het orgaan bestaande uit experten van de Federale Overheidsdienst Binnenlandse Zaken, van de Federale Overheidsdienst Economie, KMO, Middenstand en Energie en van de Federale Overheidsdienst Informatie- en Communicatietechnologie, dat belast is met het toezicht op de door de overheid aangemelde stelsels voor elektronische identificatie;

§ 2. De begrippen die in hoofdstuk 3 van deze wet voorkomen en die niet in paragraaf 1 van dit artikel worden gedefinieerd, worden begrepen in de zin van de definities van artikel 3 van verordening 910/2014.

Afdeling 2

Toepassingsgebied

Artikel 4

§ 1. Hoofdstuk 3 van deze wet is van toepassing op Belgische stelsels voor elektronisch identificatie die aangemeld werden bij de Commissie overeenkomstig artikel 9 van verordening 910/2014, de verantwoordelijken daarvan en op partijen die een elektronisch identificatiemiddel uitgeven of die een authenticatieprocedure uitvoeren in het kader van een aangemeld stelsel voor elektronische identificatie.

§ 2. Hoofdstuk 4 van deze wet is van toepassing op diensten voor elektronische identificatie waarmee toegang kan worden verkregen tot Belgische digitale overheidstoepassingen.

HOOFDSTUK 3

Grensoverschrijdende elektronische identificatie

Afdeling 1

Wederzijdse erkenning

Artikel 5

§ 1. Aan de vereiste van een Belgisch elektronisch identificatiemiddel om toegang te krijgen tot een onlinedienst aangeboden door een openbare instantie in België, is voldaan door om het even welk elektronisch identificatiemiddel uitgegeven in een andere lidstaat dat voldoet aan de voorwaarden van artikel 6 van verordening 910/2014.

§ 2. Om toegang te krijgen tot een onlinedienst aangeboden door een andere vertrouwende partij dan een openbare instantie, kan gebruik worden gemaakt van een door de Belgische overheid aangemeld stelsel voor elektronische identificatie wanneer voldaan is aan de voorwaarden gesteld door de Koning, bij in Ministerraad overlegd besluit.

4° organe de contrôle: l'organe se composant d'experts du Service public fédéral Intérieur, du Service public fédéral Économie, PME, Classes moyennes et Énergie et du Service public fédéral Technologie de l'Information et de la Communication, qui est chargé du contrôle des schémas d'identification électronique notifiés par l'Administration;

§ 2. Les concepts mentionnés dans le chapitre 3 de la présente loi et qui ne sont pas définis au paragraphe 1er du présent article, sont compris au sens des définitions de l'article 3 du règlement 910/2014.

Section 2

Champ d'application

Article 4

§ 1er. Le chapitre 3 de la présente loi s'applique aux schémas d'identification électronique belges qui ont été notifiés à la Commission conformément à l'article 9 du règlement 910/2014 ainsi qu'aux leurs responsables et aux parties qui délivrent un moyen d'authentification électronique ou qui gèrent une procédure d'authentification dans le cadre d'un schéma d'identification électronique notifié.

§ 2. Le chapitre 4 de la présente loi s'applique aux services d'identification électronique permettant d'accéder à des applications publiques numériques belges.

CHAPITRE 3

Identification électronique transfrontalière

Section 1re

Reconnaissance mutuelle

Article 5

§ 1er. L'exigence d'un moyen d'identification électronique belge pour accéder à un service en ligne offert par une instance publique en Belgique, est respectée par tout moyen d'identification électronique délivré dans un autre État membre et répondant aux conditions de l'article 6 du règlement 910/2014.

§ 2. Pour accéder à un service en ligne offert par une autre partie utilisatrice qu'une instance publique, il est possible d'utiliser un schéma d'identification électronique notifié par les autorités belges lorsque les conditions posées par le Roi, par un arrêté délibéré en Conseil des ministres, ont été respectées.

Afdeling 2

Betrouwbaarheidsniveaus

Artikel 6

§ 1. Elke Belgische openbare instantie bepaalt de betrouwbaarheidsniveaus vereist voor de toegang tot haar online diensten in overeenstemming met de niveaus vervat in artikel 8 van verordening 910/2014 en informeert hierover de federale overheidsdienst Informatie- en Communicatietechnologie.

§ 2. De federale overheidsdienst Informatie- en Communicatietechnologie bepaalt, na consultatie van het College van voorzitters van de Federale en Programmatorische Overheidsdiensten, van het College van afgevaardigd bestuurders van de instellingen van sociale zekerheid en van het College van afgevaardigd bestuurders van de federale instellingen van openbaar nut, de betrouwbaarheidsniveaus voor de bij de Commissie aan te melden elektronische identificatiemiddelen in overeenstemming met Uitvoeringsverordening (EU) 2015/1502, en zorgt voor aanmelding van één of meerdere Belgische stelsels voor elektronische identificatie overeenkomstig artikel 9 van verordening 910/2014.

Afdeling 3

Persoonsidentificatiegegevens en toegang tot het Rijksregister

Artikel 7

§ 1.De federale overheidsdienst Informatie- en Communicatietechnologie geeft in overeenstemming met artikel 11 en de bijlage van de uitvoeringsverordening (EU) 2015/1501, het minimale pakket persoonsidentificatiegegevens van de houder van een door België aangemeld elektronisch identificatiemiddel, die zich wenst te identificeren voor toegang tot een onlinedienst aangeboden in een andere lidstaat, door aan het knooppunt van die lidstaat.

§ 2. Voor de uitvoering van de verplichting vermeld in § 1, wordt de federale overheidsdienst Informatie- en Communicatietechnologie gemachtigd om de in § 1 bedoelde gegevens op te halen in het Rijksregister.

§ 3. Om te voldoen aan een verplichting van de verordening 910/2014 of één van haar uitvoeringshandelingen die de uitwisseling van bijkomende optionele persoonsidentificatiegegevens mogelijk maakt, wordt de federale overheidsdienst Informatie- en Communicatietechnologie gemachtigd, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer, om de overeenkomstige gegevens op te halen in het Rijksregister.

Section 2

Niveaux de garantie

Article 6

§ 1er. Toute instance publique belge détermine les niveaux de garantie exigés pour accéder à ses services en ligne conformément aux niveaux mentionnés à l'article 8 du règlement 910/2014 et informe le service public fédéral Technologie de l'Information et de la Communication.

§ 2. Le service public fédéral Technologie de l'Information et de la Communication détermine, après consultation du Collège des présidents des services publics fédéraux et des services publics de programmation, du Collège des administrateurs délégués des institutions de sécurité sociale et du Collège des administrateurs délégués des organismes fédéraux d'intérêt public, les niveaux de garantie pour les moyens d'identification électronique à notifier à la Commission conformément au Règlement d'exécution (UE) 2015/1502, et se charge de la notification d'un ou de plusieurs schémas d'identification électronique belges conformément à l'article 9 du règlement 910/2014.

Section 3

Données d'identification personnelle et accès au Registre national

Article 7

§ 1er. Le service public fédéral Technologie de l'Information et de la Communication transmet, conformément à l'article 11 et à l'annexe du règlement d'exécution (UE) 2015/1501, l'ensemble minimal de données d'identification personnelle du titulaire d'un moyen d'identification électronique notifié par la Belgique, qui souhaite s'identifier pour accéder à un service en ligne offert dans un autre État membre, au nœud de cet État membre.

§ 2. Pour l'exécution de l'obligation mentionnée au § 1er, le service public fédéral Technologie de l'Information et de la Communication est autorisé à obtenir du Registre national les données visées au § 1er.

§ 3. Pour satisfaire à une obligation du règlement 910/2014 ou à l'un de ses actes d'exécution qui permet l'échange de données d'identification personnelle facultatives supplémentaires, le service public fédéral Technologie de l'Information et de la Communication est autorisé, après avis de la Commission de la protection de la vie privée, à obtenir du Registre national les données correspondantes.

Afdeling 4

Toezicht en controle

Artikel 8

§ 1. Onverminderd de bepalingen van verordening 910/2014, wordt het toezichthoudend orgaan belast met het toezicht op de door de overheid aangemelde stelsels voor elektronische identificatie.

§ 2. Het toezichthoudend orgaan kan een beroep doen op de diensten van een of meer deskundigen om het te helpen in zijn toezichtsopdracht. De aangewezen deskundigen moeten financieel en organisationeel onafhankelijk zijn van de partijen die elektronische identificatiemiddelen uitgeven of die de authenticatieprocedure uitvoeren.

§ 3. Wanneer het toezichthoudend orgaan vaststelt dat een partij die een elektronisch identificatiemiddel uitgeeft of een partij die een authenticatieprocedure uitvoert zich niet houdt aan de eisen van verordening 910/2014 of van deze wet, stelt het hem in gebreke en stelt het een redelijke termijn vast in functie van de aard en de ernst van de tekortkoming, tijdens welke de in gebreke blijvende partij alle nodige maatregelen dient te hebben getroffen om die tekortkoming te verhelpen.

§ 4. Indien na afloop van de in de vorige paragraaf vermelde termijn de nodige maatregelen niet werden getroffen, kan de minister bevoegd voor digitale agenda of zijn gemachtigde, na advies van het toezichthoudend orgaan, na consultatie van het College van voorzitters van de Federale en Programmatorische Overheidsdiensten, van het College van afgevaardigd bestuurders van de instellingen van sociale zekerheid en van het College van afgevaardigd bestuurders van de federale instellingen van openbaar nut en zonder afbreuk te doen aan bijzondere regels van toepassing op elektronische identificatiemiddelen of stelsels voor elektronisch identificatie,

a) het betreffende stelsel voor elektronische identificatie of authenticatie opschorten of intrekken;

b) de partij die een elektronisch identificatiemiddel uitgeeft of die een authenticatieprocedure uitvoert te gelasten onmiddellijk vertrouwende partijen op de hoogte te brengen van de genomen maatregelen;

c) maatregelen ter verbetering van de dienstverlening opleggen ten aanzien van de in gebreke blijvende partij.

§ 5. Wanneer het toezichthoudend orgaan vaststelt dat de integriteit van een aangemeld stelsel voor elektronische identificatie of van delen daarvan geschonden is, zal de minister bevoegd voor digitale agenda of zijn gemachtigde, na consultatie van het College van voorzitters van de Federale en Programmatorische Overheidsdiensten, van het College van afgevaardigd bestuurders van de instellingen van sociale zekerheid en van het College van afgevaardigd bestuurders van de federale instellingen van openbaar nut, het volledig stelsel of de aangetaste delen daarvan intrekken of opschorten en de andere lidstaten en de Europese Commissie hiervan op de hoogte stellen conform artikel 10 van de verordening 910/2014.

Section 4

Surveillance et contrôle

Article 8

§ 1er. Sans préjudice des dispositions du règlement 910/2014, l'organe de contrôle est chargé de la surveillance des schémas d'identification électronique notifiés par l'Administration.

§ 2. L'organe de contrôle peut faire appel aux services d'un ou de plusieurs experts pour l'aider dans sa mission de surveillance. Les experts désignés doivent, financièrement et sur le plan organisationnel, être indépendants des parties qui délivrent des moyens d'identification électronique ou qui gèrent la procédure d'authentification.

§ 3. Lorsque l'organe de contrôle constate qu'une partie délivrant un moyen d'identification électronique ou une partie gérant une procédure d'authentification ne respecte pas les exigences du règlement 910/2014 ou de la présente loi, il la met en demeure et fixe un délai raisonnable en fonction de la nature et la gravité du manquement, pendant lequel la partie défaillante doit prendre toutes les mesures nécessaires pour remédier à ce manquement.

§ 4. Si, à l'issue du délai mentionné au paragraphe précédent, les mesures nécessaires n'ont pas été prises, le ministre compétent pour l'agenda numérique ou son mandataire peut, sur conseil de l'organe de contrôle, après consultation du Collège des présidents des services publics fédéraux et de programmation, du Collège des administrateurs délégués des institutions de sécurité sociale et du Collège des administrateurs délégués des organismes fédéraux d'intérêt public, et sans porter atteinte aux règles particulières applicables aux moyens d'identification électronique ou aux schémas d'identification électronique,

a) suspendre ou révoquer le schéma d'identification ou d'authentification électronique concerné;

b) sommer la partie qui délivre un moyen d'identification électronique ou qui gère une procédure d'authentification d'avertir immédiatement les parties utilisatrices des mesures prises;

c) imposer à la partie défaillante des mesures en vue de l'amélioration de la prestation de services.

§ 5. Lorsque l'organe de contrôle constate que l'intégrité d'une partie ou de la totalité d'un schéma d'identification électronique notifié est violée, le ministre compétent pour l'agenda numérique ou son mandataire, après consultation du Collège des présidents des services publics fédéraux et de programmation, du Collège des administrateurs délégués des institutions de sécurité sociale et du Collège des administrateurs délégués des organismes fédéraux d'intérêt public, révoquera ou suspendra le schéma entier ou les parties touchées et en informera les autres États membres ainsi que la Commission européenne conformément à l'article 10 du règlement 910/2014.

§ 6. De Koning kan, bij in Ministerraad overlegd besluit, de overige maatregelen bepalen die de minister, zijn gemachtigde en het toezichthoudend orgaan kunnen treffen wanneer de bepalingen van deze wet of van verordening 910/2014 niet gerespecteerd worden.

§ 7. Het toezichthoudend orgaan rapporteert jaarlijks over haar controle-activiteiten op een stelsel voor elektronische identificatie aan de autoriteiten verantwoordelijk voor die stelsels.

Afdeling 5

Samenwerking en interoperabiliteit

Artikel 9

Overeenkomstig artikel 3 van het Uitvoeringsbesluit 2015/296 van 24 februari 2015 van de Commissie tot vaststelling van procedurele voorschriften betreffende de samenwerking tussen de lidstaten op het gebied van elektronische identificatie overeenkomstig artikel 12, lid 7, van verordening 910/2014, wordt de federale overheidsdienst Informatie- en Communicatietechnologie aangewezen als één loket.

Artikel 10

De federale overheidsdienst Informatie- en Communicatietechnologie wordt aangewezen als exploitant van een knooppunt, als bedoeld in artikel 2 van Uitvoeringsverordening 2015/1501.

HOOFDSTUK 4

Elektronische identificatie voor Belgische overheidstoepassingen

Afdeling 1

Authenticatiedienst

Artikel 11

§ 1. Onverminderd de verplichtingen verbonden aan de verordening 910/2014, wordt de federale overheidsdienst voor Informatie- en Communicatietechnologie belast met het aanbieden van elektronische aanmeldingsdiensten voor overheidstoepassingen, binnen de authenticatiedienst.

§ 2. De federale overheidsdienst voor Informatie- en Communicatietechnologie zorgt voor de beschikbaarheid van de authenticatiedienst.

§ 3. Voor de uitvoering van haar opdracht van authenticatie heeft de federale overheidsdienst voor Informatie- en Communicatietechnologie het recht om het identificatienummer van de natuurlijke personen opgenomen in het Rijksregister te gebruiken.

§ 6. Le Roi peut, par un arrêté délibéré en Conseil des ministres, déterminer les autres mesures que le ministre, son mandataire et l'organe de contrôle peuvent prendre lorsque les dispositions de la présente loi ou du règlement 910/2014 ne sont pas respectées.

§ 7. L'organe de contrôle fait annuellement rapport sur ses activités de contrôle portant sur un schéma d'identification électronique aux autorités qui sont responsables de ces schémas.

Section 5

Collaboration et interopérabilité

Article 9

Conformément à l'article 3 de la Décision d'exécution (UE) 2015/296 de la Commission du 24 février 2015 établissant les modalités de coopération entre les États membres en matière d'identification électronique conformément à l'article 12, paragraphe 7, du règlement (UE) n ° 910/2014, le service public fédéral Technologie de l'Information et de la Communication est désigné comme guichet unique.

Article 10

Le service public fédéral Technologie de l'Information et de la Communication est désigné comme exploitant d'un nœud, tel que visé à l'article 2 du règlement d'exécution 2015/1501.

CHAPITRE 4

Identification électronique pour applications publiques belges

Section 1re

Service d'authentification

Article 11

§ 1er. Sans préjudice des obligations liées au règlement 910/2014, le service public fédéral Technologie de l'Information et de la Communication est chargé d'offrir des services d'identification électronique pour des applications publiques au sein du service d'authentification.

§ 2. Le service public fédéral Technologie de l'Information et de la Communication veille à la disponibilité du service d'authentification.

§ 3. Pour l'exécution de sa mission d'authentification, le service public fédéral Technologie de l'Information et de la Communication a le droit d'utiliser le numéro d'identification des personnes physiques inscrites au Registre national.

Afdeling 2

Erkenning van elektronische aanmeldingsdiensten

Artikel 12

§ 1. Andere partijen dan openbare instanties kunnen hun diensten voor elektronische identificatie, die door de federale overheidsdienst voor Informatie- en Communicatietechnologie, na consultatie van het College van voorzitters van de Federale en Programmatorische Overheidsdiensten, van het College van afgevaardigd bestuurders van de instellingen van sociale zekerheid en van het College van afgevaardigd bestuurders van de federale instellingen van openbaar nut, zijn erkend, aanbieden voor toegang tot overheidstoepassingen binnen de authenticatiedienst.

§ 2. De Koning bepaalt, bij in Ministerraad overlegd besluit, de procedure, de voorwaarden en de gevolgen van de erkenning van diensten voor elektronische identificatie voor toegang tot overheidstoepassingen, aangeboden door andere partijen dan openbare instanties, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer.

§ 3. De federale overheidsdienst voor Informatie- en Communicatietechnologie publiceert de procedure, de voorwaarden en de gevolgen van de erkenning, op de website van de authenticatiedienst.

§ 4. Wanneer nuttig laat de federale overheidsdienst voor Informatie- en Communicatietechnologie zich bij de erkenning bijstaan door deskundigen.

§ 5. De aanbieder van een erkende dienst voor elektronische identificatie wordt voor de toepassing van dit artikel beschouwd als een onderaannemer van de erkennende overheid in de zin van artikel 5, eerste lid, 3°, van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen en in die hoedanigheid gemachtigd om het rijksregisternummer te gebruiken uitsluitend voor aanbieding van de erkende dienst voor elektronische identificatie via de authenticatiedienst.

§ 6. Onverminderd de bevoegdheden en actiemogelijkheden van andere overheden of controlediensten kan de federale overheidsdienst voor Informatie- en Communicatietechnologie de aanbieders van erkende diensten voor elektronische identificatie aan een controle onderwerpen bij klacht of vermoeden van niet-overeenstemming van de dienstverlening met de goedgekeurde erkenningsvoorwaarden.

§ 7. Wanneer de federale overheidsdienst voor Informatie- en Communicatietechnologie vaststelt dat de dienstverlening niet overeenstemt met de goedgekeurde erkenningsvoorwaarden, legt hij de door de Koning, bij in Ministerraad overlegd besluit, bepaalde maatregelen op.

§ 8. De Koning kan de vergoedingsregeling bepalen voor de aanbieders van erkende diensten voor elektronische identificatie.

Section 2

Agrément de services d'identification électronique

Article 12

§ 1er. Des parties autres que des instances publiques peuvent offrir leurs services d'identification électronique, agréés par le service public fédéral Technologie de l'Information et de la Communication, après consultation du Collège des présidents des service publics fédéraux et des services publics de programmation, du Collège des administrateurs délégués des institutions de la sécurité sociale et du Collège des administrateurs délégués des organismes d'intérêt public fédéraux , pour accéder à des applications publiques au sein du service d'authentification.

§ 2. Le Roi détermine, par un arrêté délibéré en Conseil des ministres, la procédure, les conditions et les conséquences relatives à l'agrément des services d'identification électronique pour accéder à des applications publiques, offerts par des parties autres que des instances publiques, après avis de la Commission de la protection de la vie privée.

§ 3. Le service public fédéral Technologie de l'Information et de la Communication publie sur le site web du service d'authentification la procédure, les conditions et les conséquences de l'agrément.

§ 4. En cas de nécessité, le service public fédéral Technologie de l'Information et de la Communication se fait assister par des experts.

§ 5. Le fournisseur d'un service d'identification électronique agréé est, pour l'application du présent article, considéré comme un sous-traitant de l'autorité d'agrément au sens de l'article 5, alinéa 1, 3°, de la loi du 8 août 1983 organisant un Registre national des personnes physiques, et est, en cette qualité, autorisé à utiliser le numéro de Registre national exclusivement pour offrir le service d'identification électronique agréé par le biais du service d'authentification.

§ 6. Sans préjudice des compétences et possibilités d'action d'autres autorités ou services de contrôle, le service public fédéral Technologie de l'Information et de la Communication peut soumettre à un contrôle les fournisseurs de services d'identification électronique agréés en cas de plainte ou de suspicion de non-conformité du service aux conditions d'agrément approuvées.

§ 7. Lorsque le service public fédéral Technologie de l'Information et de la Communication constate que la prestation de services n'est pas conforme aux conditions d'agrément approuvées, il impose les mesures déterminées par le Roi, par un arrêté délibéré en Conseil des ministres.

§ 8. Le Roi peut déterminer le régime d'indemnités pour les fournisseurs de services d'identification électronique agréés.

Afdeling 3

Verplichtingen verbonden aan het elektronisch identificatiemiddel

Artikel 13

De houder van een elektronisch identificatiemiddel is ertoe gehouden alle nodige maatregelen te nemen om het elekronisch identificatiemiddel onder zijn exclusieve controle te houden, om diefstal, verlies of verspreiding van zijn elektronisch identificatiemiddel te voorkomen en om in geval van diefstal, verlies of verspreiding zijn elektronisch identificatiemiddel onmiddellijk te laten intrekken.

Wanneer het elektronische identificatiemiddel vervalt of ingetrokken wordt, mag de houder ervan na de vervaldatum of na intrekking het elektronisch identificatiemiddel niet meer wetens en willens gebruiken.

HOOFDSTUK 5

Inwerkingtreding

Artikel 14

De Koning bepaalt de inwerkingtreding van hoofdstuk 3 van deze wet.

Section 3

Obligations liées au moyen d'identification électronique

Article 13

Le titulaire d'un moyen d'identification électronique est tenu de prendre toutes les mesures nécessaires pour garder sous son contrôle exclusif le moyen d'identification électronique, pour prévenir le vol, la perte ou la divulgation de ce moyen d'identification électronique et pour le révoquer immédiatement en cas de vol, de perte ou de divulgation.

Lorsque le moyen d'identification électronique vient à échéance ou est révoqué, son titulaire ne peut plus l'utiliser sciemment après la date d'échéance ou la révocation.

CHAPITRE 5

Entrée en vigueur

Article 14

Le Roi détermine l'entrée en vigueur du chapitre 3 de la présente loi.

Geïntegreerde impactanalyse

Beschrijvende fiche

A. Auteur

Bevoegd regeringslid

Alexander DE CROO
Vice-eersteminister en minister van Ontwikkelingssamenwerking, Digitale Agenda, Telecommunicatie en Post

Contactpersoon beleidscel

Naam : Emmanuel Pieters

E-mail : Emmanuel.Pieters@premier.fed.be

Tel. Nr. : 02 792 99 00

Overheidsdienst

Federale Overheidsdienst Informatie- en Communicatietechnologie

Contactpersoon overheidsdienst

Naam : Samoera Jacobs

E-mail : samoera.jacobs@fedict.be

Tel. Nr. : 02 212 96 49

B. Ontwerp

Titel van de regelgeving

Voorontwerp van wet inzake elektronische identificatie

Korte beschrijving van het ontwerp van regelgeving met vermelding van de oorsprong (verdrag, richtlijn, samenwerkingsakkoord, actualiteit, …), de beoogde doelen van uitvoering.

Dit voorontwerp van wet strekt er enerzijds toe om bepalingen te voorzien die moeten toelaten verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG toe te passen voor wat hoofdstuk II aangaande elektronische identificatie betreft. Dit gedeelte van het voorontwerp betreft de Europese grensoverschrijdende context.

Dit voorontwerp van wet strekt er anderzijds toe om een juridisch kader te creëren voor elektronische identificatie voor digitale overheidstoepassingen. In het bijzonder voorziet dit voorontwerp in een wettelijke verankering van de Belgische federale authenticatiedienst en in de mogelijkheid om diensten voor elektronische identificatie te erkennen met het oog op het verkrijgen van toegang tot Belgische overheidstoepassingen. Dit gedeelte van het voorontwerp betreft de Belgische context.

Impactanalyses reeds uitgevoerd:

☐ Ja ■ Nee

C. Raadpleging over het ontwerp van regelgeving

Verplichte, facultatieve of informele raadplegingen

notificatie aan de Europese Commissie krachtens Richtlijn 98/34/EG

D. Bronnen gebruikt om de impactanalyse uit te voeren

Statistieken, referentiedocumenten, organisaties en referentiepersonen

/

Welke impact heeft het ontwerp van regelgeving op deze 21 thema's?

1. Kansarmoedebestrijding

☐ Positieve impact ☐ Negatieve impact | ■ Geen impact

2. Gelijke kansen en sociale cohesie

☐ Positieve impact ☐ Negatieve impact | ■ Geen impact

3. Gelijkheid van vrouwen en mannen

1. Op welke personen heeft het ontwerp (rechtstreeks of onrechtstreeks) een impact en wat is de naar geslacht uitgesplitste samenstelling van deze groep(en) van personen?

☐ Er zijn personen betrokken. | ■ Personen zijn niet betrokken.

Leg uit waarom:

geen onderscheid mannen/vrouwen

4. Gezondheid

☐ Positieve impact ☐ Negatieve impact | ■ Geen impact

5. Werkgelegenheid

☐ Positieve impact ☐ Negatieve impact | ■ Geen impact

6. Consumptie- en productiepatronen

☐ Positieve impact ☐ Negatieve impact | ■ Geen impact

7. Economische ontwikkeling

☐ Positieve impact ☐ Negatieve impact | ■ Geen impact

8. Investeringen

☐ Positieve impact ☐ Negatieve impact | ■ Geen impact

9. Onderzoek en ontwikkeling

■ Positieve impact ☐ Negatieve impact | ☐ Geen impact

Leg uit

de ontwikkeling van nieuwe elektronische middelen voor identificatie en authentificatie wordt gestimuleerd.

10. Kmo's

1. Welke ondernemingen zijn rechtstreeks of onrechtstreeks betrokken?

■ Er zijn ondernemingen (inclusief kmo's) betrokken. | ☐ Ondernemingen zijn niet betrokken.

Beschrijf de sector(en), het aantal ondernemingen, het % kmo's (

de elektronische middelen voor identificatie en authentificatie kunnen worden aangeleverd door ondernemingen.

2. Identificeer de positieve en negatieve impact van het ontwerp op de kmo's.

N.B. de impact op de administratieve lasten moet bij het punt 11 gedetailleerd worden

aanbod van diensten aan de overheid, innovatie

☐ Er is een negatieve impact.

11. Administratieve lasten

☒ Ondernemingen of burgers zijn betrokken. ☐ Ondernemingen of burgers zijn niet betrokken.

1. Identificeer, per betrokken doelgroep, de nodige formaliteiten en verplichtingen voor de toepassing van de regelgeving.

Huidige regelgeving	Ontwerp van regelgeving
vaak formaliteiten op papier	uitbreiden van elektronische middelen voor identificatie in België en in Europa

☐ Vink dit aan indien er formaliteiten en/of verplichtingen zijn in de huidige regelgeving.

☐ Vink dit aan indien er formaliteiten en/of verplichtingen zijn in het ontwerp van regelgeving.

12. Energie

☐ Positieve impact ☐ Negatieve impact ☒ Geen impact

13. Mobiliteit

☐ Positieve impact ☐ Negatieve impact ☒ Geen impact

14. Voeding

☐ Positieve impact ☐ Negatieve impact ☒ Geen impact

15. Klimaatverandering

☐ Positieve impact ☐ Negatieve impact ☒ Geen impact

16. Natuurlijke hulpbronnen

☐ Positieve impact ☐ Negatieve impact ☒ Geen impact

17. Buiten- en binnenlucht

☐ Positieve impact ☐ Negatieve impact ☒ Geen impact

18. Biodiversiteit

☐ Positieve impact ☐ Negatieve impact ☒ Geen impact

19. Hinder

☐ Positieve impact ☐ Negatieve impact ☒ Geen impact

20. Overheid

☒ Positieve impact ☐ Negatieve impact ☐ Geen impact

Leg uit

ruimere beschikbaarheid van de administratie voor burgers en ondernemingen via elektronische identificatie

21. Beleidscoherentie ten gunste van ontwikkeling

1. Identificeer de eventuele rechtstreekse of onrechtstreekse impact van het ontwerp op de ontwikkelingslanden op het vlak van: voedselveiligheid, gezondheid en toegang tot geneesmiddelen, waardig werk, lokale en internationale handel, inkomens en mobilisering van lokale middelen (taxatie), mobiliteit van personen, leefmilieu en klimaatverandering (mechanismen voor schone ontwikkeling), vrede en veiligheid.

☐ Impact op ontwikkelingslanden. | ■ Geen impact op ontwikkelingslanden.

Leg uit waarom:

/

Analyse d'impact intégrée

Fiche signalétique

A. Auteur

Membre du Gouvernement compétent

Alexander DE CROO

Le Vice-Premier ministre et ministre de la Coopération au développement, de l'Agenda numérique, des Télécommunications et de la Poste

Contact cellule stratégique

Nom : Emmanuel Pieters

E-mail : Emmanuel.Pieters@premier.fed.be

Téléphone : 02 792 99 00

Administration

Service Public Fédéral Technologie de l'Information et de la Communication

Contact administration

Nom : Samoera Jacobs

E-mail : samoera.jacobs@fedict.be

Téléphone : 02 212 96 49

B. Projet

Titre de la règlementation

Avant-projet de loi relative à l'identification électronique

Description succincte du projet de réglementation en mentionnant l'origine réglementaire (traités, directive, accord de coopération, actualité, …), les objectifs poursuivis et la mise en œuvre.

Le présent avant-projet de loi vise d'une part à prévoir des dispositions qui doivent permettre d'appliquer le règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, concernant le chapitre II portant sur l'identification électronique. Cette partie de l'avant-projet concerne le contexte transfrontalier européen.

Le présent avant-projet de loi vise d'autre part à créer un cadre juridique pour l'identification électronique sur des applications publiques numériques. Cet avant-projet prévoit en particulier l'ancrage légal du service fédéral d'authentification belge et la possibilité d'agréer des services d'identification électronique afin d'accéder aux applications publiques belges. Cette partie de l'avant-projet concerne le contexte belge.

Analyses d'impact déjà réalisées :

☐ Oui ■ Non

C. Consultations sur le projet de réglementation

Consultation obligatoire, facultative ou informelle

notification à la Commission Européenne conformément la Directive 98/34/EG

D. Sources utilisées pour effectuer l'analyse d'impact

Statistiques, documents, institutions et personnes de référence

/

Quel est l'impact du projet de réglementation sur ces 21 thèmes ?

1. Lutte contre la pauvreté

☐ Impact positif ☐ Impact négatif | ■ Pas d'impact

2. Égalité des chances et cohésion sociale

☐ Impact positif ☐ Impact négatif | ■ Pas d'impact

3. Égalité des femmes et des hommes

1. Quelles personnes sont (directement et indirectement) concernées par le projet et quelle est la composition sexuée de ce(s) groupe(s) de personnes ?

☐ Des personnes sont concernées. | ■ Aucune personne n'est concernée.

Expliquez pourquoi :

geen onderscheid mannen/vrouwen

4. Santé

☐ Impact positif ☐ Impact négatif | ■ Pas d'impact

5. Emploi

☐ Impact positif ☐ Impact négatif | ■ Pas d'impact

6. Modes de consommation et production

☐ Impact positif ☐ Impact négatif | ■ Pas d'impact

7. Développement économique

☐ Impact positif ☐ Impact négatif | ■ Pas d'impact

8. Investissements

☐ Impact positif ☐ Impact négatif | ■ Pas d'impact

9. Recherche et développement

■ Impact positif ☐ Impact négatif | ☐ Pas d'impact

Expliquez

le développement de nouveaux moyens électroniques d'identification et d'authentification est encouragé.

10. PME

1. Quelles entreprises sont directement et indirectement concernées ?

■ Des entreprises (dont des PME) sont concernées. | ☐ Aucune entreprise n'est concernée.

Détaillez le(s) secteur(s), le nombre d'entreprises, le % de PME (

les moyens électroniques pour identification et authentification peuvent être livrés par des entreprises.

2. Identifiez les impacts positifs et négatifs du projet sur les PME.

N.B. les impacts sur les charges administratives doivent être détaillés au thème 11

offre de services à l'administration, innovation

☐ Il y a des impacts négatifs.

11. Charges administratives

☒ Des entreprises/citoyens sont concernés. ☐ Les entreprises/citoyens ne sont pas concernés.

1. Identifiez, par groupe concerné, les formalités et les obligations nécessaires à l'application de la réglementation.

Réglementation actuelle	Réglementation en projet
souvent des formalités sur papier	élargir les moyens électroniques d'identification en Belgique et en Europe

☐ S'il y a des formalités et/ou des obligations dans la réglementation actuelle, cochez cette case.

☐ S'il y a des formalités et/ou des obligations pour la réglementation en projet, cochez cette case.

12. Énergie

☐ Impact positif ☐ Impact négatif ☒ Pas d'impact

13. Mobilité

☐ Impact positif ☐ Impact négatif ☒ Pas d'impact

14. Alimentation

☐ Impact positif ☐ Impact négatif ☒ Pas d'impact

15. Changements climatiques

☐ Impact positif ☐ Impact négatif ☒ Pas d'impact

16. Ressources naturelles

☐ Impact positif ☐ Impact négatif ☒ Pas d'impact

17. Air intérieur et extérieur

☐ Impact positif ☐ Impact négatif ☒ Pas d'impact

18. Biodiversité

☐ Impact positif ☐ Impact négatif ☒ Pas d'impact

19. Nuisances

☐ Impact positif ☐ Impact négatif ☒ Pas d'impact

20. Autorités publiques

☒ Impact positif ☐ Impact négatif ☐ Pas d'impact

Expliquez

disponibilité plus large de l'administration pour citoyens et entreprises via identification électronique

21. Cohérence des politiques en faveur du développement

1. Identifiez les éventuels impacts directs et indirects du projet sur les pays en développement dans les domaines suivants : sécurité alimentaire, santé et accès aux médicaments, travail décent, commerce local et international, revenus et mobilisations de ressources domestiques (taxation), mobilité des personnes, environnement et changements climatiques (mécanismes de développement propre), paix et sécurité.

☐ Impact sur les pays en développement. | ■ Pas d'imapct sur les pays en développement.

Expliquez pourquoi :

/

ADVIES VAN DE RAAD VAN STATE NR. 60.899/4 VAN 20 FEBRUARI 2017

Op 25 januari 2017 is de Raad van State, afdeling Wetgeving, door de vice-eersteminister en minister van Ontwikkelingssamenwerking, Digitale Agenda, Telecommunicatie en Post verzocht binnen een termijn van dertig dagen een advies te verstrekken over een voorontwerp van wet "inzake elektronische identificatie".

Het voorontwerp is door de vierde kamer onderzocht op 20 februari 2017. De kamer was samengesteld uit Pierre Liénardy, kamervoorzitter, Martine Baguet en Bernard Blero, staatsraden, Sébastien Van Drooghenbroeck en Marianne Dony, assessoren, en Colette Gigot, griffier.

Het verslag is uitgebracht door Laurence Vancrayebeck, eerste auditeur.

De overeenstemming tussen de Franse en de Nederlandse tekst van het advies is nagezien onder toezicht van Pierre Liénardy.

Het advies, waarvan de tekst hierna volgt, is gegeven op 20 februari 2017.

*

Aangezien de adviesaanvraag ingediend is op basis van artikel 84, § 1, eerste lid, 2°, van de gecoördineerde wetten op de Raad van State, beperkt de afdeling Wetgeving overeenkomstig artikel 84, § 3, van de voornoemde gecoördineerde wetten haar onderzoek tot de rechtsgrond[1*] van het voorontwerp, de bevoegdheid van de steller van de handeling en de te vervullen voorafgaande vormvereisten.

Wat deze drie punten betreft, geeft het voorontwerp aanleiding tot de volgende opmerkingen.

ALGEMENE OPMERKINGEN

1.1. Luidens artikel 2 van het voorliggende voorontwerp van wet strekt deze wet er inzonderheid toe uitvoering te geven aan "hoofdstuk II (elektronische identificatie) van verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG" (hierna "verordening (EU) nr. 910/2014" genoemd).

Overeenkomstig artikel 288, tweede alinea, van het Verdrag betreffende de werking van de Europese Unie is een verordening verbindend in al haar onderdelen en is ze rechtstreeks toepasselijk in elke lidstaat. Behoudens wanneer bij een verordening bepaalde uitvoeringsmaatregelen aan de

1* Aangezien het om een voorontwerp van wet gaat, wordt onder "rechtsgrond" de overeenstemming met de hogere rechtsnormen verstaan.

AVIS DU CONSEIL D'ÉTAT N° 60.899/4 DU 20 FÉVRIER 2017

Le 25 janvier 2017, le Conseil d'État, section de législation, a été invité par le vice-premier ministre et ministre de la Coopération au développement, de l'Agenda numérique, des Télécommunications et de la Poste à communiquer un avis, dans un délai de trente jours, sur un avant-projet de loi "relative à l'identification électronique".

L'avant-projet a été examiné par la quatrième chambre le 20 février 2017. La chambre était composée de Pierre Liénardy, président de chambre, Martine Baguet et Bernard Blero, conseillers d'État, Sébastien Van Drooghenbroeck et Marianne Dony, assesseurs, et Colette Gigot, greffier.

Le rapport a été présenté par Laurence Vancrayebeck, première auditrice.

La concordance entre la version française et la version néerlandaise a été vérifiée sous le contrôle de Pierre Liénardy.

L'avis, dont le texte suit, a été donné le 20 février 2017.

*

Comme la demande d'avis est introduite sur la base de l'article 84, § 1er, alinéa 1er, 2°, des lois coordonnées sur le Conseil d'État, la section de législation limite son examen au fondement juridique [1(*)] de l'avant-projet, à la compétence de l'auteur de l'acte ainsi qu'à l'accomplissement des formalités préalables, conformément à l'article 84, § 3, des lois coordonnées précitées.

Sur ces trois points, l'avant-projet appelle les observations suivantes.

OBSERVATIONS GÉNÉRALES

1.1. Selon l'article 2 de l'avant-projet de loi à l'examen, celle-ci a notamment pour objet "d'exécuter le chapitre II (identification électronique) du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE" (ci-après le "règlement (UE) n° 910/2014").

Conformément à l'article 288, alinéa 2, du Traité sur le fonctionnement de l'Union européenne, un règlement est obligatoire dans tous ses éléments et est directement applicable dans tout État membre. Sauf lorsqu'un règlement confie certaines mesures d'exécution aux États membres ou si le

1* S'agissant d'un avant-projet de loi, on entend par "fondement juridique" la conformité aux normes supérieures.

lidstaten worden opgedragen of de betrokken verordening enige ruimte laat voor het nemen van zulke uitvoeringsmaatregelen, betekent die rechtstreekse toepasselijkheid dat geen optreden van de lidstaten vereist is om de bepalingen ervan te integreren in hun interne rechtsorde. Bepalingen van een verordening moeten inzonderheid niet worden omgezet in het interne recht van de lidstaten. Niet alleen is een dergelijke werkwijze overbodig op het normatieve vlak aangezien ze geen nieuwe norm tot stand brengt, maar bovendien houdt ze het gevaar in dat verwarring ontstaat inzake het rechtskarakter van het in de internrechtelijke regeling opgenomen voorschrift en onder meer over de bevoegdheid van het Hof van Justitie van de Europese Unie om kennis te nemen van alle betwistingen in verband met de voorschriften van de verordening. Ook kan deze werkwijze verwarring doen ontstaan over het tijdstip van inwerkingtreding van de betrokken normen.[2]

Het overnemen van bepalingen van een EU-verordening in een internrechtelijke regeling kan dan ook alleen worden gedoogd in zoverre dat noodzakelijk is voor de leesbaarheid van eventuele internrechtelijke uitvoeringsmaatregelen, in welk geval een verwijzing naar de betreffende bepaling van de verordening het aangewezen middel zal zijn om de aard van die bepaling herkenbaar te houden ("Overeenkomstig artikel … van verordening …").[3]

1.2. Sommige bepalingen van het voorontwerp strekken er inderdaad toe ervoor te zorgen dat verordening (EU) nr. 910/2014 volledig uitwerking kan hebben, maar dat betekent nog niet dat het voorontwerp de gehele verordening "uitvoert". Teneinde elk misverstand op dat punt te voorkomen, moet het gebruik van het werkwoord "uitvoeren" zowel in het voorliggende dispositief als in de memorie van toelichting en in de artikelsgewijze bespreking geweerd worden. De memorie van toelichting en de artikelsgewijze bespreking moeten herzien worden zodat duidelijk blijkt in welk opzicht het voorliggende dispositief de volledige tenuitvoerlegging van de verordening in het Belgische interne recht regelt.

Zo ook mag niet vermeld worden dat het voorontwerp iets "toevoegt" aan verordening (EU) nr. 910/2014, aangezien deze op zich volstaat. Het zou beter zijn die "toevoegingen" eveneens te kaderen in de volledige tenuitvoerlegging van de verordening en, indien nodig, uit te leggen waarom het dispositief van het voorontwerp, daar waar dit verder reikt dan de verordening, toch geen inbreuk maakt op die verordening.

Het voorontwerp voorziet daarentegen niet in een aantal bepalingen die evenwel noodzakelijk zouden kunnen zijn om verordening (EU) nr. 910/2014 concreet ten uitvoer te leggen in het Belgische interne recht.

règlement concerné laisse une certaine marge pour prendre pareilles mesures, une telle applicabilité directe signifie qu'il n'est pas nécessaire que les États membres interviennent en vue d'intégrer les dispositions du règlement dans leur ordre juridique interne. Les dispositions d'un règlement ne doivent notamment pas être transposées dans le droit interne des États membres. Un tel procédé est non seulement superflu d'un point de vue normatif, dès lors qu'il ne crée aucune nouvelle norme, mais il risque également de semer la confusion quant à la nature juridique de la règle incorporée dans le régime de droit interne et, notamment, en ce qui concerne la compétence de la Cour de justice de l'Union européenne à connaître de tout litige relatif aux règles définies par le règlement. Ce procédé risque aussi de créer une équivoque en ce qui concerne le moment de l'entrée en vigueur des normes concernées [2].

L'intégration de dispositions d'un règlement de l'Union européenne dans une disposition de droit interne ne peut dès lors être tolérée que dans la mesure où elle est nécessaire à la lisibilité d'éventuelles mesures d'exécution de droit interne, auquel cas un renvoi à la disposition concernée du règlement ("Conformément à l'article ... du règlement …") constituera le moyen approprié pour identifier la nature de cette disposition [3].

1.2. Certes, certaines dispositions de l'avant-projet ont pour objet de permettre au règlement (UE) n° 910/2014 de sortir tous ses effets. Ce faisant, il n'"exécute" pas pour autant le règlement dans son ensemble. Pour éviter tout malentendu sur ce point, il convient de proscrire, tant dans le dispositif à l'examen que dans l'exposé des motifs et le commentaire des articles, l'utilisation du verbe "exécuter". L'exposé des motifs et le commentaire des articles seront revus pour faire apparaitre en quoi le dispositif à l'examen organise la pleine mise en œuvre du règlement en droit interne belge.

Dans le même ordre d'idées, il n'y a pas lieu d'indiquer que l'avant-projet "ajoute" au règlement (UE) n° 910/2014, celui-ci se suffisant à lui-même. Il serait plus judicieux de placer ces "ajouts" dans la même perspective de la pleine mise en œuvre du règlement et, si nécessaire, d'expliciter en quoi le dispositif de l'avant-projet qui irait au-delà du règlement n'enfreint cependant pas celui-ci.

En revanche, l'avant-projet ne prévoit pas certains dispositifs qui pourraient cependant être requis pour assurer la concrétisation, en droit interne belge, du règlement (UE) n° 910/2014.

---

2 HvJ 7 februari 1973, *Commissie v. Italië*, punt 17, *Jur.* 1973, 101.

3 Zie inzonderheid advies 54.817/VR, gegeven op 13 januari 2014 over een voorontwerp van wet 'houdende instemming met het Samenwerkingsakkoord van 27 februari 2014 tussen de Federale Staat, het Vlaamse Gewest, Waalse Gewest en het Brussels Hoofdstedelijk Gewest betreffende de oprichting van een vergunningscoördinerend en -faciliterend comité voor trans-Europese energie-infrastructuurprojecten, ter uitvoering van verordening (EU) nr. 347/2013".

2 C.J.U.E., 7 février 1973, (Commission c. Italie), point 17, *Jur.* 1973, p. 101.

3 Voir not. l'avis 54.817/VR, donné le 13 janvier 2014, sur un avant-projet de loi "portant assentiment à l'Accord de coopération du 27 février 2014 entre l'État fédéral, la Région flamande, la Région wallonne et la Région de Bruxelles-Capitale relatif à la création d'un comité de coordination et de facilitation pour l'octroi des autorisations pour des projets d'infrastructures énergétiques transeuropéennes, en exécution du Règlement (UE) n° 347/2013".

Dat is het geval met het toezichthoudend orgaan, waarvan de oprichting en de samenstelling moeten worden geregeld, aangezien de steller van het voorontwerp de bedoeling zou hebben om aan dat orgaan bijzondere prerogatieven te verlenen zodat het gemachtigd zou zijn om verplichtingen op te leggen aan derden.

Zo wordt bij het voorontwerp ook geen enkele sanctie opgelegd, terwijl het naar luid van artikel 16 van verordening (EU) nr. 910/2014 aan de lidstaten staat om "de voorschriften inzake de sancties die van toepassing zijn op inbreuken op deze verordening" vast te stellen. De vraag rijst of de steller van het voorontwerp van oordeel is dat binnen het geheel van de Belgische rechtsregels een toereikende sanctieregeling voorhanden is om aan die verplichting te voldoen. Indien dat het geval is, moet in de memorie van toelichting gepreciseerd worden waaruit die regeling bestaat en waarom ze toereikend geacht wordt. Zo niet, moet het voorontwerp aangevuld worden.

2. De artikelen 6, 7 en 9 tot 12 hebben betrekking op federale overheidsdiensten die bij naam genoemd worden, en meer bepaald op de federale overheidsdienst Informatie- en Communicatietechnologie, waaraan verschillende uitvoeringstaken rechtstreeks opgedragen worden.

Er wordt op gewezen dat, luidens artikel 37 van de Grondwet, de federale uitvoerende macht, zoals zij door de Grondwet is geregeld, bij de Koning berust. Daaruit volgt dat de regeling van de organisatie en de werkwijze van de bestuursdiensten zaak is van de Koning. Van dit beginsel kan de wetgever slechts afwijken wanneer daartoe een dwingende reden bestaat, bijvoorbeeld wanneer een hogere rechtsnorm daartoe zou verplichten of wanneer dit ingrijpen zijn reden vindt in het vrijwaren van de rechten van de burger.[4]

Het is derhalve in beginsel de werkwijze waarbij de met de uitvoering van wetsbepalingen belaste organen op een generieke wijze worden aangewezen, die moet worden gevolgd, bijvoorbeeld door de woorden "door de Koning aangewezen dienst" te gebruiken.

3. De opzet van het voorontwerp behoort dan ook grondig te worden herzien teneinde met deze opmerkingen rekening te houden. Met het oog daarop zullen in de bijzondere opmerkingen nog preciseringen gegeven worden.

Il en va ainsi de l'organe de contrôle qui doit être prévu, quant à sa création et composition, dès lors qu'il serait de l'intention de l'auteur de l'avant-projet de lui conférer des prérogatives particulières en manière telle que cet organe serait habilité à imposer des obligations à des tiers.

De même, l'avant-projet ne comporte aucune sanction alors qu'aux termes de l'article 16 du règlement (UE) n° 910/2014, il appartient aux États membres de fixer "le régime des sanctions applicables aux violations du règlement". La question se pose de savoir si l'auteur de l'avant-projet estime que l'arsenal juridique belge compte déjà à l'heure actuelle un régime de sanctions suffisant pour satisfaire à cette obligation. Si tel est le cas, l'exposé des motifs précisera en quoi consiste cet arsenal et en quoi il est jugé suffisant. À défaut, l'avant-projet sera complété.

2. Les articles 6, 7 et 9 à 12 visent des services publics fédéraux nommément cités, en particulier le Service public fédéral Technologie de l'Information et de la Communication, auquel sont confiées directement plusieurs missions d'exécution.

Il est rappelé que selon l'article 37 de la Constitution, le pouvoir exécutif fédéral, tel qu'il est réglé par la Constitution, appartient au Roi. Il en découle qu'il revient au Roi de régler l'organisation et le fonctionnement de l'administration. Le législateur ne peut déroger à ce principe que pour une raison impérieuse, par exemple lorsqu'une norme supérieure l'y oblige ou lorsque cette intervention est motivée par la préservation des droits du citoyen [4].

Par conséquent, la méthode à suivre en principe consiste à désigner de manière générique les organes chargés de l'exécution des dispositions légales, par exemple en utilisant les termes "service désigné par le Roi".

3. En conclusion, l'avant-projet sera fondamentalement revu sur le plan de sa conception pour tenir compte de ces observations. Dans cette perspective, des précisions seront par ailleurs apportées dans les observations particulières.

[4] Zie inzonderheid advies 54.929/3, gegeven op 29 januari 2014 over een voorontwerp dat geleid heeft tot de wet van 25 april 2014 "tot aanpassing in de fiscale wetgeving van de benamingen van de administraties van de Federale Overheidsdienst Financiën en houdende verscheidene andere wetswijzigingen" (*Parl.St.* Kamer 2013-14, nr. 3420, 24-26).

[4] Voir notamment l'avis 54.929/3 donné le 29 janvier 2014, sur un avant-projet devenu la loi du 25 avril 2014 "adaptant dans la législation fiscale les dénominations des administrations du Service public fédéral Finances et portant diverses autres modifications législatives" (*Doc. parl.,* Chambre, 2013-2014, n° 3420, pp. 24-26).

BIJZONDERE OPMERKINGEN

Dispositief

Artikel 2

Artikel 2 van het voorontwerp strekt er alleen toe de twee hoofdlijnen van de inhoud van het ontworpen dispositief te schetsen. Gelet op algemene opmerking 1, behoort een hoofdstuk van verordening (EU) nr. 910/2014 bovendien niet als zodanig uitgevoerd worden.

Om die redenen is de bepaling zinloos en dient ze te vervallen.

Artikel 3

1. In artikel 3, § 1, 4°, is er sprake van een toezichthoudend orgaan "bestaande uit experten van de Federale Overheidsdienst Binnenlandse Zaken, van de Federale Overheidsdienst Economie, KMO, Middenstand en Energie en van de Federale Overheidsdienst Informatie- en Communicatietechnologie." Het zou belast zijn met het "toezicht op de door de overheid aangemelde stelsels voor elektronische identificatie."[5]

In beginsel worden de nadere regels voor de samenstelling en de taken van een orgaan dat wordt opgericht, niet opgenomen in de bepaling waarin het orgaan wordt gedefinieerd. Het is dan ook beter zich er in artikel 3, § 1, 4°, toe te bepalen het toezichthoudend orgaan te definiëren als "het orgaan bedoeld in artikel 8" en het principe van de oprichting en de samenstelling ervan op te nemen in artikel 8, dat meer bepaald de taken van dat orgaan bepaalt.

Wat de samenstelling betreft, mag, gelet op algemene opmerking 2, niet worden gepreciseerd uit welke federale overheidsdiensten de "experten" afkomstig zijn. Aangezien het *in casu* gaat om het aanwijzen van ambtenaren met een zekere expertise op een bepaald domein, en niet om externe experten, is het raadzaam om geen gebruik te maken van het woord "expert" dat verder in de Franse tekst van het voorontwerp trouwens in een andere betekenis gebezigd wordt.[6]

Artikel 3, § 1, 4°, behoort dienovereenkomstig herzien te worden.

OBSERVATIONS PARTICULIÈRES

Dispositif

Article 2

L'article 2 de l'avant-projet n'a d'autre objet que de décrire les deux axes du contenu du dispositif en projet. Par ailleurs, compte tenu de l'observation générale n° 1, il n'y a pas lieu d'exécuter, comme tel, un chapitre du règlement (UE) n° 910/2014.

Pour ces motifs, la disposition est inutile et sera omise.

Article 3

1. L'article 3, § 1er, 4°, fait mention d'un organe de contrôle "composé d'experts du Service public fédéral Intérieur, du Service public fédéral Économie, PME, Classes moyennes et Énergie et du Service public fédéral Technologie de l'Information et de la Communication". Il serait chargé "du contrôle des schémas d'identification électronique notifiés par l'Administration" [5].

Ce n'est en principe pas dans la disposition qui le définit que l'on précise les modalités de composition et les missions d'un organe que l'on crée. Mieux vaut dès lors, à l'article 3, § 1er, 4°, se contenter de définir l'organe de contrôle comme étant "l'organe visé à l'article 8", et inscrire à l'article 8 – qui précise notamment les missions de cet organe – le principe de sa création et sa composition.

Quant à la composition, compte tenu de l'observation générale n° 2, il n'y a pas lieu de préciser de quels services publics fédéraux sont issus les "experts". Comme il s'agit en l'espèce de désigner des fonctionnaires ayant une certaine expertise dans le domaine et non des experts extérieurs, mieux vaut éviter le terme "expert", qui est par ailleurs utilisé dans la suite de l'avant-projet dans un autre sens [6].

L'article 3, § 1er, 4°, sera revu en conséquence.

5 Verordening (EU) nr. 910/2014 voorziet weliswaar niet uitdrukkelijk in de oprichting van een dergelijk toezichthoudend orgaan, maar zoals te lezen staat in de bespreking van het artikel, "uit artikel 9, 1, b) van verordening 910/2014 volgt de plicht voor lidstaten om [in] een toezichtregeling te voorzien voor aangemelde stelsels voor elektronische identificatie".

6 Zie de artikelen 8 en 12.

5 Si la création d'un tel organe de contrôle n'est pas expressément prévue par le règlement (UE) n° 910/2014, comme l'indique le commentaire de l'article, "l'obligation pour les États membres de prévoir un régime de contrôle pour les schémas d'identification électronique notifiés découle de l'article 9.1, b) du règlement 910/2014".

6 Voir les articles 8 et 12.

2. In hoofdstuk 3 van het voorontwerp wordt gebruikgemaakt van begrippen die gedefinieerd zijn in artikel 2 van uitvoeringsverordening (EU) nr. 2015/1501[7] ("knooppunt", "exploitant van een knooppunt"). Er moet bijgevolg ook naar die bepaling verwezen worden. Aangezien in hoofdstuk 4 van het voorontwerp van wet dezelfde terminologie wordt gebruikt als in Europese regelgeving ("elektronische identificatie", "elektronisch identificatiemiddel"), moet voorts ook naar de definities vervat in die regelgeving verwezen worden voor wat betreft de begrippen die in hoofdstuk 4 gebruikt worden.

Artikel 3, § 2, behoort dienovereenkomstig te worden herzien.

Artikel 4

Artikel 4 strekt er enkel toe het toepassingsgebied van de hoofdstukken 3 en 4 van het voorontwerp te bepalen. Aangezien hoofdstuk 3 duidelijk deel uitmaakt van het dispositief dat de tenuitvoerlegging van de verordening mogelijk maakt, is het overbodig dat in artikel 4, § 1, te preciseren. Aangezien het toepassingsgebied van hoofdstuk 4 vastgelegd wordt in artikel 11, § 1, is artikel 4, § 2, eveneens overbodig.

Artikel 4 dient te vervallen.

Artikel 5

1. Artikel 5, § 1, van het voorontwerp luidt als volgt:

"Aan de vereiste van een Belgisch elektronisch identificatiemiddel om toegang te krijgen tot een onlinedienst aangeboden door een openbare instantie in België, is voldaan door om het even welk elektronisch identificatiemiddel uitgegeven in een andere lidstaat dat voldoet aan de voorwaarden van artikel 6 van verordening 910/2014".

Het betreft een bepaling die ertoe strekt om op algemene wijze te voorzien in de evenwaardigheid van de Belgische elektronische identificatiemiddelen en die welke uitgegeven worden door andere lidstaten en voldoen aan de voorwaarden vastgelegd in artikel 6 van verordening (EU) nr. 910/2014. Die ontworpen bepaling is niet meer dan een parafrase van artikel 6.1 van verordening (EU) nr. 910/2014 en dient dan ook, gelet op algemene opmerking 1, te vervallen.

2. Bij artikel 5, § 2, van het voorontwerp wordt de mogelijkheid ten uitvoer gelegd die geboden wordt bij artikel 7, f), tweede alinea, van verordening (EU) nr. 910/2014, welke bepaling luidt als volgt:

"Voor andere vertrouwende partijen dan openbare instanties mag de aanmeldende lidstaat voorwaarden stellen voor toegang tot die authenticatie. Grensoverschrijdende

[7] Uitvoeringsverordening (EU) 2015/1501 van de Commissie van 8 september 2015 "betreffende het interoperabiliteitskader bedoeld in artikel 12, lid 8, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt".

2. Le chapitre 3 de l'avant-projet utilise des concepts qui sont définis à l'article 2 du règlement d'exécution (UE) 2015/1501 [7] ("nœud", "opérateur de nœud"). Il convient dès lors de renvoyer également à cette disposition. Par ailleurs, dès lors que le chapitre 4 de l'avant-projet de loi utilise la même terminologie ("identification électronique", "moyen d'identification électronique"), il y a lieu de renvoyer également aux définitions contenues dans les normes européennes pour ce qui concerne les concepts utilisés au chapitre 4.

L'article 3, § 2, sera revu en conséquence.

Article 4

L'article 4 se donne pour seul objet de définir le champ d'application des chapitres 3 et 4 de l'avant-projet. Or, le chapitre 3 se plaçant clairement dans la mise en place du dispositif permettant la mise œuvre du règlement, il est inutile de le préciser à l'article 4, § 1er. De même, l'article 11, § 1er, déterminant le champ d'application du chapitre 4, l'article 4, § 2, est superflu.

L'article 4 sera omis.

Article 5

1. Selon l'article 5, § 1er, de l'avant-projet,

"L'exigence d'un moyen d'identification électronique belge pour accéder à un service en ligne offert par une instance publique en Belgique est respectée par tout moyen d'identification électronique délivré dans un autre État membre et répondant aux conditions de l'article 6 du règlement 910/2014".

Il s'agit d'une disposition qui vise à établir, de manière générale, une équivalence entre les moyens d'identification électroniques belges et ceux qui sont délivrés par d'autres États membres et qui répondent aux conditions fixées à l'article 6 du règlement (UE) n° 910/2014. Ce faisant, la disposition en projet ne fait que paraphraser l'article 6.1 du règlement (UE) n° 910/2014 et, compte tenu de l'observation générale n° 1, elle doit dès lors être omise.

2. L'article 5, § 2, de l'avant-projet met en œuvre une faculté offerte par l'article 7, f), alinéa 2, du règlement (UE) n° 910/2014, selon lequel:

"Pour les parties utilisatrices autres que des organismes du secteur public, l'État membre notifiant peut définir les conditions d'accès à cette authentification. Cette authentification

[7] Règlement d'exécution (UE) 2015/1501 de la Commission du 8 septembre 2015 "sur le cadre d'interopérabilité visé à l'article 12, paragraphe 8, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur".

authenticatie is kosteloos wanneer zij wordt uitgevoerd voor een door een openbare instantie verleende onlinedienst."

Wanneer de mogelijkheid die bij deze bepaling geboden wordt ten uitvoer wordt gelegd, mag niet afgeweken worden van hetgeen bepaald wordt in verordening (EU) nr. 910/2014. Om alle verwarring te voorkomen zou *in casu* de ontworpen bepaling een verwijzing moeten bevatten naar artikel 7, f), tweede alinea, van dezelfde verordening en zou daarin ook dezelfde terminologie gebezigd moeten worden. Aldus zou in de Franse tekst niet "*instance publique*" (niet nader gedefinieerd) geschreven moeten worden, maar wel "*organisme du secteur public*", welk begrip gedefineerd wordt in artikel 3.7 van verordening (EU) nr. 910/2014.[8]

In de bespreking van het artikel staat voorts het volgende: "Omdat hier allicht een impact is op het vlak van persoonsgegevens zal hierover het advies gevraagd worden van de Commissie voor de bescherming van de persoonlijke levenssfeer".[9] Dat zulk een advies vereist is, blijkt niet uit de ontworpen bepaling. Dat gebrek aan overeenstemming moet worden verholpen.

Artikel 6

Door te bepalen dat "[e]lke Belgische openbare instantie (...) de betrouwbaarheidsniveaus vereist voor de toegang tot haar online diensten (bepaalt)", wordt in artikel 6, § 1, van het voorontwerp, een bepaling weergegeven die voortvloeit uit verordening (EU) nr. 910/2014, hetgeen niet kan worden toegestaan, zoals ook hiervoor wordt uitgelegd in algemene opmerking 1. De verplichting om de federale overheidsdienst Informatie- en Communicatietechnologie (lees: "de door de Koning aangewezen dienst") te informeren vloeit daarenboven automatisch voort uit artikel 9 van het voorontwerp waarin bepaald wordt dat deze overheidsdienst wordt aangewezen als "één loket".

Artikel 6, § 2, regelt in hoofdzaak kwesties die de interne organisatie van het bestuur betreffen. Het hoort dan ook niet thuis in een wettelijke regeling.

Om die redenen behoort het artikel te vervallen.

transfrontalière est fournie gratuitement lorsqu'elle est effectuée en liaison avec un service en ligne fourni par un organisme du secteur public".

Il convient, lorsque la faculté offerte par cette disposition est mise en œuvre, de s'en tenir à ce que prévoit le règlement (UE) n° 910/2014. En l'espèce, pour éviter toute confusion, la disposition en projet devrait comprendre une référence à l'article 7, f), alinéa 2, du même règlement et utiliser la même terminologie. Ainsi, il convient non pas de mentionner l'"instance publique" (non autrement définie), mais bien l'"organisme du secteur public", notion qui est définie à l'article 3.7 du règlement (UE) n° 910/2014 [8].

Par ailleurs, le commentaire de l'article précise que "comme l'impact en la matière sur les données à caractère est personnel est évident, on demandera à ce sujet l'avis de la Commission de la protection de la vie privée" [9]. L'exigence d'un tel avis n'apparait pas dans le dispositif en projet. Cette discordance doit être levée.

Article 6

En prévoyant que "[t]oute instance publique belge détermine les niveaux de garantie exigés pour accéder à ses services en ligne", l'article 6, § 1er, de l'avant-projet reproduit un dispositif qui résulte du règlement (UE) n° 910/2014, ce qui ne peut être admis comme cela est exposé plus haut à l'observation générale n° 1. Par ailleurs, l'obligation imposée d'avertir le Service public fédéral Technologies de l'Information et de la Communication (lire "le service désigné par Roi") découle naturellement de l'article 9 de l'avant-projet qui est relatif au "guichet unique".

L'article 6, § 2, règle essentiellement des questions d'organisation interne à l'administration. Il n'a donc pas sa place dans un dispositif légal.

Pour ces raisons, l'article sera omis.

---

8 *"Un État, une autorité régionale ou locale, un organisme de droit public ou une association constituée d'une ou de plusieurs de ces autorités ou d'un ou de plusieurs de ces organismes de droit public, ou une entité privée mandatée par au moins un ou une de ces autorités, organismes, ou associations pour fournir des services publics lorsqu'elle agit en vertu de ce mandat".*

9 Daarmee wordt wellicht gevolg gegeven aan advies 48/2016 van de Commissie voor de bescherming van de persoonlijke levenssfeer waarin deze van oordeel was dat "het (…) momenteel voor de Commissie onmogelijk (is) in te schatten wat voor impact dit zal hebben op het vlak van verwerking van persoonsgegevens" en het volgende gesteld heeft: "M.b.t. dit koninklijk besluit wordt dan ook best voorafgaandelijk het advies van de Commissie ingewonnen". (blz. 5).

8 "Un État, une autorité régionale ou locale, un organisme de droit public ou une association constituée d'une ou de plusieurs de ces autorités ou d'un ou de plusieurs de ces organismes de droit public, ou une entité privée mandatée par au moins un ou une de ces autorités, organismes, ou associations pour fournir des services publics lorsqu'elle agit en vertu de ce mandat".

9 Ceci fait sans doute écho à l'avis 48/2016 de la Commission de protection de la vie privée dans lequel elle estimait impossible actuellement d'évaluer l'impact que cela aurait au niveau du traitement de données à caractère personnel et précisait ce qui suit: "Il serait dès lors préférable de recueillir préalablement l'avis de la Commission concernant cet arrêté royal" (p. 5).

Artikel 7

Paragraaf 1 strekt er enkel toe te bepalen welke overheidsdienst belast wordt met de verplichting om bepaalde gegevens door te geven aan het "knooppunt" van een andere lidstaat. Gelet op algemene opmerking 2 dient deze bepaling te vervallen.

Mede rekening houdend met diezelfde algemene opmerking 2 behoren in de paragrafen 2 en 3, die behouden moeten blijven in zoverre ze de Koning de noodzakelijke machtiging verlenen om de dienst die hij aanwijst toegang te geven tot de gegevens van het Rijksregister, de woorden "federale overheidsdienst Informatie- en Communicatietechnologie" te worden geschrapt en vervangen te worden door de woorden "door de Koning aangewezen dienst".

Artikel 7 moet dienovereenkomstig worden herzien.

Artikel 8

1. Artikel 10 van verordening (EU) nr. 910/2014 bepaalt welke maatregelen (opschorting, intrekking) van toepassing zijn wanneer de betrouwbaarheid van de grensoverschrijdende authenticatie in het gedrang komt door een "inbreuk op" of een gedeeltelijke schending van de integriteit van het stelsel voor elektronische identificatie of de onlineauthenticatie.

Artikel 8, § 5, van het voorontwerp heeft betrekking op dat geval, terwijl in de paragrafen 3, 4 en 6 op meer algemene wijze voorzien wordt in de mogelijkheid om een hele reeks maatregelen op te leggen aan de partij die een elektronische identificatiemiddel uitgeeft of die een authenticatieprocedure uitvoert, ingeval de voorschriften van verordening (EU) nr. 910/2014 of van de ontworpen wet niet worden nageleefd.

Aangezien verordening (EU) nr. 910/2014 onder meer strekt tot "het wegnemen van bestaande belemmeringen voor het grensoverschrijdende gebruik van elektronische identificatiemiddelen die in de lidstaten worden gebruikt"[10], lijkt deze de lidstaten niet te machtigen om, naast de strafmaatregelen waarin voorzien wordt bij artikel 10 van verordening (EU) nr. 910/2014 in geval van inbreuk op de beveiliging, ook in andere maatregelen te voorzien om iedere schending van de bepalingen van deze verordening te bestraffen (en lijkt deze al helemaal niet de Koning te machtigen om andere aanvullende maatregelen vast te stellen).

Daarentegen staat niets eraan in de weg dat in de ontworpen tekst voorzien wordt in maatregelen ter voorbereiding van de maatregelen tot opschorting of intrekking of in bijkomstige maatregelen in dat verband.

Artikel 8, §§ 3, 4 en 6, moet derhalve in het licht hiervan opnieuw worden onderzocht.

2. Gelet op algemene opmerking 2, behoort niet verwezen te worden naar de minister of diens gemachtigde, maar

[10] Overweging 12.

Article 7

Le paragraphe 1er vise uniquement à préciser quel est le service public qui sera chargé de l'obligation de transmettre certaines données au "nœud" d'un autre État membre. Compte tenu de l'observation générale n° 2, cette disposition sera omise.

Compte tenu également de cette même observation générale n° 2, les paragraphes 2 et 3, s'ils doivent être maintenus en tant qu'ils investissent le Roi de l'habilitation nécessaire à autoriser le service qu'il désigne d'avoir accès aux données du Registre national, doivent être expurgés des mots "Service public fédéral Technologies de l'Information et de la Communication" pour les remplacer par ceux de "service désigné par le Roi".

L'article 7 sera revu en conséquence.

Article 8

1. L'article 10 du règlement (UE) n° 910/2014 prévoit les mesures applicables (suspension, révocation, retrait) lorsque la fiabilité de l'authentification transfrontalière est affectée par une atteinte ou une altération partielle du schéma d'identification électronique ou de l'authentification en ligne.

L'article 8, § 5, de l'avant-projet concerne cette hypothèse, tandis que les paragraphes 3, 4 et 6 permettent, de manière plus générale, d'imposer toute une série de mesures à la partie qui délivre un moyen d'identification électronique ou qui gère une procédure d'authentification, en cas de non respect des exigences du règlement (UE) n° 910/2014 ou de la loi en projet.

Dès lors que le règlement (UE) n° 910/2014 a notamment pour objectif "de lever les obstacles existants à l'utilisation transfrontalière des moyens d'identification électronique employés dans les États membres pour s'identifier" [10], il ne semble pas autoriser les États membres à prévoir, complémentairement aux mesures de sanctions prévues par l'article 10 du règlement (UE) n° 910/2014 en cas d'atteinte à la sécurité, d'autres mesures visant à sanctionner tout manquement aux dispositions de ce règlement (et encore moins à autoriser le Roi à déterminer d'autres mesures complémentaires).

Par contre, rien ne s'oppose à ce que le texte en projet prévoie des mesures préparatoires ou accessoires aux mesures de suspension, de révocation ou de retrait.

L'article 8, §§ 3, 4 et 6, sera réexaminé en conséquence.

2. Compte tenu de l'observation générale n° 2, il n'y a pas lieu de viser le ministre ou son "mandataire", mais bien

[10] Considérant 12.

wel naar de Koning die zijn bevoegdheden eventueel kan overdragen.

Afdeling 2

De Nederlandse tekst van het opschrift moet worden gecorrigeerd

Artikel 12

1. Artikel 12 strekt ertoe de erkenning mogelijk te maken van diensten voor elektronische identificatie die ontwikkeld zijn door instellingen uit de privésector om toegang te krijgen tot digitale overheidstoepassingen in België (§ 1). De aanbieders van deze diensten zouden eventueel in aanmerking kunnen komen voor een vergoedingsregeling die door de Koning moet worden bepaald (§ 8).

In de bespreking van het artikel wordt de context van de bepaling geschetst en de verschillende bestaande mogelijkheden van identificatie genoemd die steunen op het gebruik van de elektronische identiteitskaart, waarvoor het gebruik van een kaartlezer vereist is:

"In een snel evoluerende digitale wereld waar de burger op verschillende manieren en vanop verschillende toestellen, met inbegrip van mobiele toestellen zoals tablets en smartphones, in contact wenst te treden met de overheid, staat de overheid voor de uitdaging het groeiend aanbod van digitale overheidstoepassingen eveneens open te stellen voor deze nieuwe mobiele toestellen".

In de bespreking van het artikel wordt in dat verband gesteld dat de dienst die door de Koning wordt aangewezen "authenticatiediensten, al dan niet gebaseerd op mobiele middelen voor elektronische identificatie, kan erkennen zodat deze erkende diensten burgers toegang mogen geven via de federale authenticatiedienst tot digitale overheidstoepassingen in België".

Aangezien het gaat om de ontwikkeling van digitale toepassingen voor het bestuur die later ook ter beschikking worden gesteld van de burgers, stelt de afdeling Wetgeving zich vragen bij de werkwijze waarin wordt voorzien. Indien het bestuur de levering van een toepassing vraagt en het de prijs daarvoor betaalt, moet die transactie plaatsvinden in het kader van de wetgeving op de openbare aanbestedingen. In dat geval vraagt de afdeling Wetgeving zich af of "de door de Koning vast te stellen voorwaarden voor erkenning", waaronder "minstens (de) functionele en technische kenmerken, (het) respect voor de persoonlijke levenssfeer en (de) invulling van veiligheidsvereisten, (het) dienstverleningsbeheer en (de) juridische en economische kenmerken", niet de technische voorschriften uitmaken van een bestek.

Om uitleg gevraagd over een "eventuele vergoedingsregeling voor betaling van erkende diensten voor elektronische identificatie (...) vastgesteld door de Koning", heeft de gemachtigde ambtenaar inzonderheid de volgende toelichtingen verstrekt:

le Roi, à qui il appartiendra de déléguer éventuellement ses compétences.

Section 2

La version néerlandaise de l'intitulé doit être corrigée

Article 12

1. L'article 12 tend à permettre d'agréer des services d'identification électronique développés par des organismes du secteur privé afin d'accéder à des applications publiques numériques en Belgique (§ 1er). Les fournisseurs de ces services pourraient éventuellement bénéficier d'un régime d'indemnités à déterminer par le Roi (§ 8).

Le commentaire de l'article évoque le contexte de la disposition, à côté des différentes possibilités d'identification existantes basées sur l'utilisation de la carte d'identité électronique, laquelle nécessite l'usage d'un lecteur de carte:

"Dans un monde numérique en évolution rapide dans lequel le citoyen souhaite entrer en contact avec l'administration de différentes manières et à partir de plusieurs appareils, y compris des appareils mobiles comme des tablettes et des smartphones, l'administration doit relever le défi consistant à ouvrir à ces nouveaux appareils mobiles l'offre croissante d'applications publiques numériques".

Le commentaire de l'article précise à cet égard que le service désigné par le Roi pourra "agréer des services d'authentification basés ou non sur des moyens d'identification électronique mobiles afin que ces services agréés puissent permettre aux citoyens d'accéder via le service fédéral d'authentification aux applications publiques numériques en Belgique".

S'agissant de la conception d'applications numériques développées pour l'administration et ultérieurement mises à la disposition des citoyens, la section de législation s'interroge sur le mécanisme mis en place. Si l'administration sollicite la fourniture d'une application et qu'elle en paie le prix, l'opération est appelée à se réaliser dans la cadre de la législation sur les marchés publics. Dans cette hypothèse, la section de législation se demande si les "conditions d'agrément à fixer par le Roi", parmi lesquelles "au moins […] les caractéristiques fonctionnelles et techniques, le respect de la vie privée et d'exigences de sécurité, la gestion des services ainsi que les caractéristiques juridiques et économiques" sont concernées, ne constituent pas les spécifications techniques d'un cahier spécial des charges.

Interrogée sur le mécanisme d'"éventuel régime d'indemnités relatif au paiement des services d'identification électronique agréés […] fixé par le Roi", la fonctionnaire déléguée a notamment fourni les explications suivantes:

"De erkende aanbieders van diensten voor elektronische identificatie kunnen vergoed worden.

De vergoedingsregeling krijgt vorm als een dienstenconcessie, niet als een overheidsopdracht.

De eventuele vergoeding gebeurt aan de hand van het aantal door de erkende aanbieder verrichte aanmeldingen in het vorige jaar. De vergoedingsregeling moet zich beperken tot een minimale onkostenvergoeding. De aanbieder is blootgesteld aan de vraag door de eindgebruikers die niet zeker is. Er is dus een mogelijkheid dat gedane investeringen en kosten niet kunnen worden terugverdiend.

Dit houdt in dat het substantieel exploitatierisico bij de erkende aanbieder ligt".

In dit andere geval lijkt het ter beschikking stellen van "digitale overheidstoepassingen" te geschieden op grond van concessies die vallen onder de regeling van de wet van 17 juni 2016 "betreffende de concessieovereenkomsten".

De bespreking van de thans voorliggende bepaling is onduidelijk op dat punt. Het antwoord op de vraag wie de vergoedingen moet betalen waarvan sprake in artikel 12, § 8, van het voorontwerp en aan wie deze worden betaald, is eveneens onduidelijk.

Indien het ten slotte gaat om digitale toepassingen die ontwikkeld werden door economische actoren die door de gebruikers worden vergoed, herinnert de afdeling Wetgeving eraan dat de invoering van een erkenningsregeling in overeenstemming moet zijn met richtlijn 2006/123/EG van het Europees Parlement en de Raad van 12 december 2006 "betreffende diensten op de interne markt" en met de bepalingen waarbij die richtlijn is omgezet in het Belgisch recht.

Het staat aan de steller van het voorontwerp om in de bespreking van het artikel de aard van de regeling die hij wil invoeren te preciseren. Zodra die keuze is gemaakt, dient hij deze ook te toetsen aan de regels van het Gemeenschapsrecht, waarbij hij erop dient toe te zien dat hij de verordeningen die van toepassing zouden zijn niet overneemt of parafraseert.

De tekst moet opnieuw worden onderzocht en dienovereenkomstig worden gesteld.

2. Teneinde elke mogelijke verwarring te vermijden behoren in de Franse tekst van de paragrafen 1 en 2 de woorden "*instances publiques*" vervangen te worden door de woorden "*organismes du secteur public*".

De griffier, *Le président,*

Colette GIGOT Pierre LIÉNARDY

"De erkende aanbieders van diensten voor elektronische identificatie kunnen vergoed worden.

De vergoedingsregeling krijgt vorm als een dienstenconcessie, niet als een overheidsopdracht.

De eventuele vergoeding gebeurt aan de hand van het aantal door de erkende aanbieder verrichte aanmeldingen in het vorige jaar. De vergoedingsregeling moet zich beperken tot een minimale onkostenvergoeding. De aanbieder is blootgesteld aan de vraag door de eindgebruikers die niet zeker is. Er is dus een mogelijkheid dat gedane investeringen en kosten niet kunnen worden terugverdiend.

Dit houdt in dat het substantieel exploitatierisico bij de erkende aanbieder ligt".

Dans cette autre hypothèse, la mise à disposition "d'applications publiques numériques" semble fonctionner sur la base de concessions, lesquelles sont soumises au régime de la loi du 17 juin 2016 "relative aux contrats de concession".

Le commentaire de la disposition examinée est peu clair à cet égard. Est aussi incertaine la réponse à la question de savoir à charge de qui sont mises les indemnités dont il est question à l'article 12, § 8, de l'avant-projet et à qui elles sont payées.

Enfin, s'il s'agit d'applications numériques développées par des agents économiques rémunérés par les utilisateurs, la section de législation rappelle que la mise en place d'un régime d'agrément doit être conforme à la directive 2006/123/CE du Parlement européen et du Conseil du 12 décembre 2006 "relative aux services dans le marché intérieur" et aux dispositions qui en ont assuré la transposition en droit belge.

Il appartient à l'auteur de l'avant-projet de préciser dans le commentaire de l'article la nature du mécanisme qu'il entend mettre en place. Une fois ce choix opéré, il lui appartient encore de vérifier sa conformité aux règles de droit communautaire, tout en veillant à ne pas recopier ou paraphraser les règlements qui seraient applicables.

Le texte sera réexaminé et rédigé en conséquence.

2. Aux paragraphes 1er et 2, pour éviter toute source de confusion, les termes "instances publiques" seront remplacés par les termes "organismes du secteur public".

Le greffier, *De voorzitter,*

Colette GIGOT Pierre LIÉNARDY

WETSONTWERP

FILIP,

KONING DER BELGEN,

Aan allen die nu zijn en hierna wezen zullen,
ONZE GROET.

Op de voordracht van de vice-eersteminister en minister van Ontwikkelingssamenwerking, Digitale Agenda, Telecom en Post,

HEBBEN WIJ BESLOTEN EN BESLUITEN WIJ:

De vice-eersteminister en minister van Ontwikkelingssamenwerking, Digitale Agenda, Telecom en Post is ermee belast het ontwerp van wet waarvan de tekst hierna volgt, in Onze naam bij de Kamer van volksvertegenwoordigers in te dienen:

HOOFDSTUK 1

Algemene bepaling

Artikel 1

Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.

HOOFDSTUK 2

Definities

Afdeling 1

Definities

Artikel 2

§ 1. Voor de toepassing van deze wet en de uitvoeringsbesluiten wordt verstaan onder:

1° verordening 910/2014: de verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG;

2° uitvoeringsverordening (EU) 2015/1501: de uitvoeringsverordening (EU) 2015/1501 van de Commissie van

PROJET DE LOI

PHILIPPE,

ROI DES BELGES,

À tous, présents et à venir,
SALUT.

Sur la proposition du vice-premier ministre et ministre de la Coopération au développement, de l'Agenda numérique, des Télécom et de la Poste,

NOUS AVONS ARRÊTÉ ET ARRÊTONS:

Le vice-premier ministre et ministre de la Coopération au développement, de l'Agenda numérique, des Télécom et de la Poste est chargé de déposer à la Chambre des représentants le projet de loi dont la teneur suit:

CHAPITRE 1ER

Disposition générale

Article 1er

La présente loi règle une matière visée à l'article 74 de la Constitution.

CHAPITRE 2

Définitions

Section 1re

Définitions

Article 2

§ 1er. Pour l'application de la présente loi et des arrêtés d'exécution, on entend par:

1° règlement 910/2014: le règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE;

2° règlement d'exécution (UE) 2015/1501: le règlement d'exécution (UE) 2015/1501 de la Commission du

8 september 2015 betreffende het interoperabiliteitskader bedoeld in artikel 12, lid 8, van verordening 910/2014;

3° uitvoeringsverordening (EU) 2015/1502: de uitvoeringsverordening (EU) 2015/1502 van 8 september 2015 van de Commissie tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3 van verordening 910/2014;

4° toezichthoudend orgaan: het orgaan bedoeld in artikel 6;

5° knooppunt: een aansluitpunt zoals gedefinieerd in artikel 2, 1° van de uitvoeringsverordening (EU) 2015/1501;

§ 2. De begrippen die in hoofdstuk 3 van deze wet voorkomen en die niet in paragraaf 1 van dit artikel worden gedefinieerd, worden begrepen in de zin van de definities van artikel 3 van verordening 910/2014.

HOOFDSTUK 3

Grensoverschrijdende elektronische identificatie

Afdeling 1

Wederzijdse erkenning

Artikel 3

Om overeenkomstig artikel 7, f), lid 2 van verordening 910/2014 toegang te krijgen tot een onlinedienst aangeboden door een andere vertrouwende partij dan een openbare instantie, kan gebruik worden gemaakt van een door de Belgische overheid aangemeld stelsel voor elektronische identificatie wanneer voldaan is aan de voorwaarden gesteld door de Koning, bij in Ministerraad overlegd besluit.

Afdeling 2

Betrouwbaarheidsniveaus

Artikel 4

§ 1. Met het oog op de wederzijdse erkenning bedoeld in artikel 6 van verordening 910/2014, bepaalt elke Belgische openbare instantie de betrouwbaarheidsniveaus vereist voor de toegang tot haar online diensten in overeenstemming met de niveaus vervat in artikel 8 van verordening 910/2014 en informeert hierover de de instantie aangeduid door de Koning.

8 septembre 2015 sur le cadre d'interopérabilité visé à l'article 12, paragraphe 8, du règlement 910/2014;

3° règlement d'exécution (UE) 2015/1502: le règlement d'exécution (UE) 2015/1502 de la Commission européenne du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3, du règlement 910/2014;

4° organe de contrôle: l'organe visé à l'article 6;

5° nœud: un point de connexion tel que défini à l'article 2, 1° de l'arrêté d'exécution (UE) 2015/1501;

§ 2. Les concepts mentionnés au chapitre 3 de la présente loi et qui ne sont pas définis au paragraphe 1er du présent article, sont compris au sens des définitions de l'article 3 du règlement 910/2014.

CHAPITRE 3

Identification électronique transfrontalière

Section 1re

Reconnaissance mutuelle

Article 3

Pour accéder, conformément à l'article 7, f), alinéa 2, du règlement 910/2014, à un service en ligne offert par une partie utilisatrice autre qu'un organisme du secteur public, il est possible d'utiliser un schéma d'identification électronique notifié par l'Administration belge lorsque les conditions posées par le Roi, par un arrêté délibéré en Conseil des ministres, ont été respectées.

Section 2

Niveaux de garantie

Article 4

§ 1er. En vue de la reconnaissance mutuelle visée à l'article 6 du règlement 910/2014, toute instance publique belge détermine les niveaux de garantie exigés pour accéder à ses services en ligne conformément aux niveaux mentionnés à l'article 8 du règlement 910/2014 et en informe l'instance désignée par le Roi.

§ 2. De instantie bedoeld in § 1 bepaalt, na consultatie van vertegenwoordigers van het College van voorzitters van de federale en programmatorische overheidsdiensten, van het College van afgevaardigd bestuurders van de instellingen van sociale zekerheid en van het College van afgevaardigd bestuurders van de federale instellingen van openbaar nut, de betrouwbaarheidsniveaus voor de bij de Commissie aan te melden elektronische identificatiemiddelen in overeenstemming met uitvoeringsverordening (EU) 2015/1502, en zorgt voor aanmelding van één of meerdere Belgische stelsels voor elektronische identificatie overeenkomstig artikel 9 van verordening 910/2014.

Afdeling 3

Persoonsidentificatiegegevens en toegang tot het Rijksregister

Artikel 5

§ 1. De Koning duidt de instantie aan die, in overeenstemming met artikel 11 en de bijlage van de uitvoeringsverordening (EU) 2015/1501, het minimale pakket persoonsidentificatiegegevens van de houder van een door België aangemeld elektronisch identificatiemiddel, die zich wenst te identificeren voor toegang tot een onlinedienst aangeboden in een andere lidstaat, doorgeeft aan het knooppunt van die lidstaat.

§ 2. De instantie vermeld in § 1 wordt voor de uitvoering van de verplichting vermeld in § 1, gemachtigd om de in § 1 bedoelde gegevens op te halen in het Rijksregister.

§ 3. Om te voldoen aan een verplichting van de verordening 910/2014 of één van haar uitvoeringshandelingen die de uitwisseling van bijkomende optionele persoonsidentificatiegegevens mogelijk maakt, wordt de instantie bedoeld in § 1, gemachtigd, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer, om de overeenkomstige gegevens op te halen in het Rijksregister.

Afdeling 4

Toezicht en controle

Artikel 6

§ 1. Het toezichthoudend orgaan bestaat uit vertegenwoordigers met de nodige deskundigheid en kwalificaties inzake elektronische identificatie, aangeduid door minstens drie verschillende overheidsdiensten, en is belast met het toezicht op de door de overheid

§ 2. L'instance visée au § 1er détermine, après consultation de représentants du Collège des présidents des services publics fédéraux et des services publics de programmation, du Collège des administrateurs délégués des institutions de sécurité sociale et du Collège des administrateurs délégués des organismes fédéraux d'intérêt public, les niveaux de garantie pour les moyens d'identification électronique à notifier à la Commission conformément au règlement d'exécution (UE) 2015/1502, et se charge de la notification d'un ou de plusieurs schémas d'identification électronique belges conformément à l'article 9 du règlement 910/2014.

Section 3

Données d'identification personnelle et accès au Registre national

Article 5

§ 1er. Le Roi désigne l'instance qui, conformément à l'article 11 et à l'annexe du règlement d'exécution (UE) 2015/1501, transmet l'ensemble minimal de données d'identification personnelle du titulaire d'un moyen d'identification électronique notifié par la Belgique, qui souhaite s'identifier pour accéder à un service en ligne offert dans un autre État membre, au nœud de cet État membre.

§ 2. Pour l'exécution de l'obligation mentionnée au § 1er, l'instance visée au § 1er est autorisée à obtenir du Registre national les données visées au § 1er.

§ 3. Pour satisfaire à une obligation du règlement 910/2014 ou à l'un de ses actes d'exécution qui permet l'échange de données d'identification personnelle facultatives supplémentaires, l'instance visée au § 1er est autorisée, après avis de la Commission de la protection de la vie privée, à obtenir du Registre national les données correspondantes.

Section 4

Surveillance et contrôle

Article 6

§ 1er. L'organe de contrôle se compose de représentants disposant de l'expertise et des qualifications nécessaires en matière d'identification électronique, qui sont désignés par au moins trois services publics différents, et est chargé de contrôler les schémas

aangemelde stelsels voor elektronische identificatie en met het nemen van de maatregelen zoals bedoeld in artikel 10 van verordening 910/2014.

§ 2. Het toezichthoudend orgaan kan een beroep doen op de diensten van een of meer deskundigen om het te helpen in zijn toezichtsopdracht. De aangewezen deskundigen moeten financieel en organisationeel onafhankelijk zijn van de partijen die elektronische identificatiemiddelen uitgeven of die de authenticatieprocedure uitvoeren.

§ 3. Tijdens de termijn van 3 maanden bedoeld in artikel 10, lid 3 van verordening 910/2014 kan het toezichthoudend orgaan herstellingsmaatregelen opleggen en bevestiging eisen van het herstel van de inbreuk of schending, door middel van een externe audit.

§ 4. Wanneer het toezichthoudend orgaan vaststelt dat de integriteit van een aangemeld stelsel voor elektronische identificatie of van delen daarvan geschonden is, zal de instantie aangeduid door de Koning, het volledig stelsel of de aangetaste delen daarvan intrekken of opschorten en de andere lidstaten en de Europese Commissie hiervan op de hoogte stellen conform artikel 10 van de verordening 910/2014.

§ 5. Het toezichthoudend orgaan rapporteert jaarlijks over haar toezichtsopdracht aan de autoriteiten verantwoordelijk voor de aangemelde stelsels voor elektronische identificatie.

Afdeling 5

Samenwerking en interoperabiliteit

Artikel 7

De Koning duidt de instantie aan die fungeert als één loket, overeenkomstig artikel 3 van het uitvoeringsbesluit 2015/296 van 24 februari 2015 van de Commissie tot vaststelling van procedurele voorschriften betreffende de samenwerking tussen de lidstaten op het gebied van elektronische identificatie overeenkomstig artikel 12, lid 7, van verordening 910/2014.

Artikel 8

De Koning duidt de instantie aan die fungeert als exploitant van een knooppunt, zoals bedoeld in artikel 2 van uitvoeringsverordening 2015/1501.

d'identification électronique notifiés par l'Administration et de prendre les mesures telles que visées à l'article 10 du règlement 910/2014.

§ 2. L'organe de contrôle peut faire appel aux services d'un ou de plusieurs experts pour l'aider dans sa mission de contrôle. Les experts désignés doivent, financièrement et sur le plan organisationnel, être indépendants des parties qui délivrent des moyens d'identification électronique ou qui gèrent la procédure d'authentification.

§ 3. Pendant le délai de 3 mois visé à l'article 10, alinéa 3, du règlement 910/2014, l'organe de contrôle peut imposer des mesures de réparation et exiger la confirmation de la réparation de l'atteinte ou de l'altération, au moyen d'un audit externe.

§ 4. Lorsque l'organe de contrôle constate que l'intégrité d'une partie ou de la totalité d'un schéma d'identification électronique notifié est violée, l'instance désignée par le Roi, révoquera ou suspendra le schéma entier ou les parties touchées et en informera les autres États membres ainsi que la Commission européenne conformément à l'article 10 du règlement 910/2014.

§ 5. L'organe de contrôle fait annuellement rapport sur sa mission de contrôle aux autorités responsables des schémas d'identification électronique notifiés.

Section 5

Collaboration et interopérabilité

Article 7

Le Roi désigne l'instance faisant office de guichet unique, conformément à l'article 3 de la décision d'exécution (UE) 2015/296 de la Commission du 24 février 2015 établissant les modalités de coopération entre les États membres en matière d'identification électronique conformément à l'article 12, paragraphe 7, du règlement (UE) n ° 910/2014.

Article 8

Le Roi désigne l'instance faisant office d'exploitant d'un nœud, tel que visé à l'article 2 du règlement d'exécution 2015/1501.

HOOFDSTUK 4

Elektronische identificatie voor Belgische overheidstoepassingen

Afdeling 1

Authenticatiedienst

Artikel 9

§ 1. Onverminderd de verplichtingen verbonden aan de verordening 910/2014, wordt de Federale overheidsdienst Beleid en Ondersteuning belast met het aanbieden van elektronische aanmeldingsdiensten voor overheidstoepassingen binnen de authenticatiedienst.

§ 2. De Federale overheidsdienst Beleid en Ondersteuning zorgt voor de beschikbaarheid van de authenticatiedienst.

§ 3. Voor de uitvoering van haar opdracht van authenticatie heeft de Federale overheidsdienst Beleid en Ondersteuning het recht om het identificatienummer van de natuurlijke personen opgenomen in het Rijksregister te gebruiken.

Afdeling 2

Erkenning van diensten voor elektronische identificatie

Artikel 10

§ 1. Andere partijen dan openbare instanties kunnen hun diensten voor elektronische identificatie, die door de Federale overheidsdienst Beleid en Ondersteuning, na consultatie van vertegenwoordigers van het College van voorzitters van de federale en programmatorische overheidsdiensten, van het College van afgevaardigd bestuurders van de instellingen van sociale zekerheid en van het College van afgevaardigd bestuurders van de federale instellingen van openbaar nut, zijn erkend, aanbieden voor toegang tot overheidstoepassingen binnen de authenticatiedienst.

§ 2. De Koning bepaalt, bij in Ministerraad overlegd besluit, de procedure, de voorwaarden en de gevolgen van de erkenning van diensten voor elektronische identificatie voor toegang tot overheidstoepassingen, aangeboden door andere partijen dan openbare instanties, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer.

CHAPITRE 4

Identification électronique pour applications publiques belges

Section 1re

Service d'authentification

Article 9

§ 1er. Sans préjudice des obligations liées au règlement 910/2014, le service public fédéral Stratégie et Appui est chargé d'offrir des services d'identification électronique pour des applications publiques au sein du service d'authentification.

§ 2. Le service public fédéral Stratégie et Appui veille à la disponibilité du service d'authentification.

§ 3. Pour l'exécution de sa mission d'authentification, le service public fédéral Stratégie et Appui a le droit d'utiliser le numéro d'identification des personnes physiques inscrites au Registre national.

Section 2

Agrément de services d'identification électronique

Article 10

§ 1er. Des parties autres que des organismes du secteur public peuvent offrir leurs services d'identification électronique, agréés par le Service public fédéral Stratégie et Appui, après consultation de représentants du Collège des présidents des service publics fédéraux et des services publics de programmation, du Collège des administrateurs délégués des institutions de la sécurité sociale et du Collège des administrateurs délégués des organismes d'intérêt public fédéraux, pour accéder à des applications publiques au sein du service d'authentification.

§ 2. Le Roi détermine, par un arrêté délibéré en Conseil des ministres, la procédure, les conditions et les conséquences relatives à l'agrément des services d'identification électronique pour accéder à des applications publiques, offerts par des parties autres que des organismes du secteur public, après avis de la Commission de la protection de la vie privée.

§ 3. De Federale overheidsdienst Beleid en Ondersteuning publiceert de procedure, de voorwaarden en de gevolgen van de erkenning, op de website van de authenticatiedienst.

§ 4. Wanneer nuttig laat de Federale overheidsdienst Beleid en Ondersteuning zich bij de erkenning bijstaan door deskundigen.

§ 5. De aanbieder van een erkende dienst voor elektronische identificatie wordt voor de toepassing van dit artikel beschouwd als een onderaannemer van de erkennende overheid in de zin van artikel 5, eerste lid, 3°, van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen en in die hoedanigheid gemachtigd om het rijksregisternummer te gebruiken uitsluitend voor aanbieding van de erkende dienst voor elektronische identificatie via de authenticatiedienst.

§ 6. Onverminderd de bevoegdheden en actiemogelijkheden van andere overheden of controlediensten kan de Federale overheidsdienst Beleid en Ondersteuning de aanbieders van erkende diensten voor elektronische identificatie aan een controle onderwerpen bij klacht of vermoeden van niet-overeenstemming van de dienstverlening met de goedgekeurde erkenningsvoorwaarden.

§ 7. Wanneer de Federale overheidsdienst Beleid en Ondersteuning vaststelt dat de dienstverlening niet overeenstemt met de goedgekeurde erkenningsvoorwaarden, legt zij de door de Koning bepaalde maatregelen op.

§ 8. De Koning kan de vergoedingsregeling bepalen voor de vergoeding die de erkennende overheid betaalt aan de aanbieders van de erkende diensten voor elektronische identificatie.

Afdeling 3

Verplichtingen verbonden aan het elektronisch identificatiemiddel

Artikel 11

De houder van een elektronisch identificatiemiddel is ertoe gehouden alle nodige maatregelen te nemen om het elektronisch identificatiemiddel onder zijn exclusieve controle te houden, om diefstal, verlies of verspreiding van zijn elektronisch identificatiemiddel te voorkomen en om in geval van diefstal, verlies of verspreiding zijn elektronisch identificatiemiddel onmiddellijk te laten intrekken.

§ 3. Le service public fédéral Stratégie et Appui publie sur le site web du service d'authentification la procédure, les conditions et les conséquences de l'agrément.

§ 4. En cas de nécessité, le service public fédéral Stratégie et Appui se fait assister par des experts.

§ 5. Le fournisseur d'un service d'identification électronique agréé est, pour l'application du présent article, considéré comme un sous-traitant de l'autorité d'agrément au sens de l'article 5, alinéa 1, 3°, de la loi du 8 août 1983 organisant un Registre national des personnes physiques, et est, en cette qualité, autorisé à utiliser le numéro de Registre national exclusivement pour offrir le service d'identification électronique agréé par le biais du service d'authentification.

§ 6. Sans préjudice des compétences et possibilités d'action d'autres autorités ou services de contrôle, le service public fédéral Stratégie et Appui peut soumettre à un contrôle les fournisseurs de services d'identification électronique agréés en cas de plainte ou de suspicion de non-conformité du service aux conditions d'agrément approuvées.

§ 7. Lorsque le Service public fédéral Stratégie et Appui constate que la prestation de services n'est pas conforme aux conditions d'agrément approuvées, il impose les mesures déterminées par le Roi.

§ 8. Le Roi peut déterminer le régime d'indemnités à payer par l'autorité d'agrément aux fournisseurs de services d'identification électronique agréés.

Section 3

Obligations liées au moyen d'identification électronique

Article 11

Le titulaire d'un moyen d'identification électronique est tenu de prendre toutes les mesures nécessaires pour garder sous son contrôle exclusif le moyen d'identification électronique, pour prévenir le vol, la perte ou la divulgation de ce moyen d'identification électronique et pour le révoquer immédiatement en cas de vol, de perte ou de divulgation.

Wanneer het elektronische identificatiemiddel vervalt of ingetrokken wordt, mag de houder ervan na de vervaldatum of na intrekking het elektronisch identificatiemiddel niet meer wetens en willens gebruiken.

HOOFDSTUK 5

Inwerkingtreding

Artikel 12

De Koning bepaalt de inwerkingtreding van hoofdstuk 3 van deze wet.

Gegeven te Brussel, 6 juni 2017

FILIP

VAN KONINGSWEGE :

De vice-eersteminister en minister van Ontwikkelingssamenwerking, Digitale Agenda, Telecommunicatie en Post,

Alexander DE CROO

Lorsque le moyen d'identification électronique vient à échéance ou est révoqué, son titulaire ne peut plus l'utiliser sciemment après la date d'échéance ou la révocation.

CHAPITRE 5

Entrée en vigueur

Article 12

Le Roi détermine l'entrée en vigueur du chapitre 3 de la présente loi.

Donné à Bruxelles, le 6 juin 2017

PHILIPPE

PAR LE ROI :

Le vice-premier ministre et ministre de la Coopération au développement, de l'Agenda numérique, des Télécommunications et de la Poste,

Alexander DE CROO

Advies nr 48/2016 van 21 september 2016

Betreft: advies m.b.t. het voorontwerp van wet inzake elektronische identificatie (CO-A-2016-032)

De Commissie voor de bescherming van de persoonlijke levenssfeer;

Gelet op de wet van 8 december 1992 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* (hierna WVP), inzonderheid artikel 29;

Gelet op het verzoek om advies van de heer Jan DEPREST, voorzitter van de Federale Overheidsdienst ICT, ontvangen op 13/05/2016;

Gelet op de aangepaste teksten van het voorontwerp ontvangen op 25/05/2016, 13/07/2016 en 14/09/2016 en gelet op de bijkomende toelichting, ontvangen op 22/08/2016;

Gelet op het verslag van de heer Ivan VANDERMEERSCH;

Brengt op 21 september 2016 het volgend advies uit:

VOORAFGAANDE OPMERKING

De Commissie vestigt er de aandacht op dat er recent nieuwe Europese regelgeving inzake de bescherming persoonsgegevens werd uitgevaardigd: de algemene Verordening betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en de Richtlijn voor Politie en Justitie. Deze teksten verschenen in het Europese Publicatieblad van 4 mei 2016[1].

De verordening, meestal GDPR (general data protection regulation) genaamd, is van kracht geworden twintig dagen na publicatie, nl. op 24 mei 2016 en wordt, twee jaar later, automatisch van toepassing: 25 mei 2018. De richtlijn voor politie en justitie moet via nationale wetgeving omgezet worden tegen uiterlijk 6 mei 2018.

Voor de Verordening betekent dit dat vanaf 24 mei 2016, en gedurende de termijn van twee jaar voor de tenuitvoerlegging, op de lidstaten enerzijds een positieve verplichting rust om alle nodige uitvoeringsbepalingen te nemen en anderzijds ook een negatieve verplichting, de zogenaamde "onthoudingsplicht". Laatstgenoemde plicht houdt in dat er geen nationale wetgeving mag worden uitgevaardigd die het door de Verordening beoogde resultaat ernstig in gevaar zou brengen. Ook voor de Richtlijn gelden gelijkaardige principes.

Het verdient dan ook aanbeveling om desgevallend nu reeds op deze teksten te anticiperen. En het is in de eerste plaats aan de adviesaanvrager(s) om hier rekening mee te houden in zijn (hun) voorstellen of ontwerpen. De Commissie heeft in onderhavig advies, in de mate van het mogelijke en onder voorbehoud van mogelijke bijkomende toekomstige standpunten, alvast gewaakt over de hoger geschetste negatieve verplichting.

I. CONTEXT

1. Het voorontwerp van wet inzake elektronische identificatie, hierna het voorontwerp, omvat 2 luiken. Het eerste luik bevat een aantal maatregelen die nodig zijn om hoofdstuk II toe te passen van de verordening (EU) nr. 910/2014 van 23 juli 2014 van het Europees Parlement en de Raad

[1] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)

Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad

http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=OJ:L:2016:119:TOC

http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC)

betreffende de elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van de Richtlijn 1999/93/EG, (hierna de verordening 910/2014).

2. In het tweede luik wordt, voor wat België betreft, de elektronische identificatie voor overheidstoepassingen juridisch onderbouwd.

3. Elektronische identificatie geschiedt via digitale systemen en gaat gepaard met de geautomatiseerde verwerking van persoonsgegevens. De bepalingen van de WVP zijn er dus van toepassing. De analyse beperkt zich tot de artikelen welke aanleiding geven tot de verwerking van persoonsgegevens.

II. ONDERZOEK TEN GRONDE

A. TOEPASSING VAN HOOFDSTUK II VAN DE VERORDENING 910/2014

Algemeen

4. Om van elektronische diensten gebruik te kunnen maken, is meestal een elektronische identificatie en authenticatie vereist. Deze laatsten vormen een struikelblok voor het grensoverschrijdend gebruik van elektronische diensten omdat een burger zijn elektronische identificatiemiddel (hierna EIM) niet kan gebruiken omdat zijn nationaal stelsel voor elektronische identificatie en authenticatie niet in de andere lidstaten is erkend. De verordening 910/2014 wil dit obstakel, alleszins voor wat identificatie en authenticatie t.o.v. openbare sector betreft, uit de wereld helpen. Hoofdstuk II bepaalt hoe dat zal gebeuren, namelijk door een systeem van verplichte wederzijdse erkenning van EIM uit te werken[1]. De aldus erkende buitenlandse EIM moeten ongehinderd in België kunnen worden gebruikt. In uitvoeringsverordeningen worden meer gedetailleerde regels vastgelegd met het oog op de concrete tenuitvoerlegging van dit systeem van wederzijdse erkenningen. Ter illustratie:

a) De uitvoeringsverordening (EU) nr. 2015/1501 handelt over het zogenaamde "interoperabiliteitskader" (dat tot doel heeft de interoperabiliteit te waarborgen van de stelsels voor elektronische identificatie die de lidstaten bij de Europese Commissie aanmelden). Deze uitvoeringsverordening legt ook regels vast betreffende de beveiliging van de gegevens en legt hierbij een belangrijke verantwoordelijkheid bij de zogenaamde "knooppunten"[2].

---

[1] Artikel 7 van de verordening 910/2014 bevat de voorwaarden waaraan een stelsel voor elektronische identificatie moet voldoen om in aanmerking te komen voor aanmelding bij de Europese Commissie. Uiterlijk een jaar na de bekendmaking door de Europese Commissie van de aangemelde stelsels voor elektronische identificatie, moeten deze worden erkend (artikelen 6.1 en 9.2 van de verordening 910/2014).

[2] In België neemt Fedict de rol van "knooppunt" op zich (artikel 10 voorontwerp).

b) In de uitvoeringsverordening (EU) nr. 2015/1502 zijn minimale technische specificaties, normen en procedures vastgelegd aan de hand waarvan het betrouwbaarheidsniveau van een EIM kan worden bepaald. Deze uitvoeringsverordening bevat ook regels inzake 'aanvraag en registratie', 'bewijs en identificatie van identiteit', 'uitgifte en activering'.

5. De Commissie stelt verder vast dat in het kader van cross-border identificatie en authenticatie, niet het Rijksregisternummer maar de STORK-ID (aangemaakt op basis van het Rijksregisternummer) meegestuurd wordt. Aldus de bijkomende informatie vanwege de steller van het voorontwerp, die de Commissie op 22 augustus 2016 ontving, is België op dit vlak geen alleenstaand geval en werkt elk Europees land met een uniek transnationaal nummer om zijn burgers te identificeren in een transnationale context[3]. Om het onderscheid tussen het gebruik van een uniek nummer in de cross-border identificatie en intra-border identificatie duidelijk te maken, wordt de memorie best aangevuld met de bijkomende informatie die de steller van het voorontwerp dienaangaande op 22 augustus 2016 aan de Commissie verstrekte.

Artikel 5, § 1, voorontwerp

6. Eigenlijk is dit een louter wetstechnische ingreep waardoor alle Belgische regelgeving die het gebruik van Belgische EIM voorschrijft om toegang te krijgen tot een elektronische dienst, in overeenstemming wordt gebracht met de verordening 910/2014, zonder dat individuele bepalingen van de Belgische regelgeving moeten worden aangepast. Ingevolge deze bepaling zullen erkende buitenlandse EIM met hetzelfde betrouwbaarheidsniveau als het Belgische EIM, moeten worden toegelaten.

7. Gelet op de bepalingen van de verordening 910/2014 enerzijds en het feit dat de equivalentie beperkt is tot EIM met hetzelfde betrouwbaarheidsniveau als datgene vereist door de Belgische regelgeving anderzijds, roept dit geen specifieke WVP-problemen op. Louter volledigheidshalve vestigt de Commissie er de aandacht op dat erover moet worden gewaakt dat de veiligheid van de keten via dewelke het identificatie- en authenticatieproces aan de hand van het buitenlands EIM geschiedt, wordt verzekerd en dat er een volledig auditspoor beschikbaar is. Dit vereist dat alle schakels in de keten kunnen worden opgespoord en dat er afspraken en/of garanties tussen alle schakels in de keten worden gemaakt (circles of trust).

---

[3] Op de vraag of een dergelijk systeem in ons land niet tot een ongelijke behandeling leidt omdat Belgen 'intern' verplicht worden om hun rijksregisternummer te verstrekken terwijl dit bij cross-border identificatie niet het geval is, antwoordt de steller het volgende: *"Iedereen die in het Rijksregister is opgenomen wordt door de gemachtigde Belgische instanties op unieke wijze geïdentificeerd aan de hand van het rijksregisternummer. Diezelfde personen worden in een Europese, transnationale context geïdentificeerd aan de hand van een afgeleid nummer. Het gaat dus om dezelfde mensen die in een andere context op een andere manier worden geïdentificeerd. (...) Deze werkwijze geldt voor elke persoon op dezelfde wijze (binnen België Rijksregisternummer, buiten België en binnen EU op een andere manier) (...)".*

Artikel 5, § 2, voorontwerp

8. Overweging 17 – heeft betrekking op artikel 7, f), tweede lid van de verordening 910/2014 - spoort de lidstaten aan om de privé-sector aan te moedigen gebruik te maken van aangemelde EIM.

9. Artikel 5, § 2, van het voorontwerp maakt gebruik van de mogelijkheid die artikel 7, f), tweede lid, van de verordening 910/2014 biedt, namelijk om het benutten door de privé-sector van aangemelde EIM te onderwerpen aan voorwaarden. De Koning wordt belast met het vaststellen van deze voorwaarden.

10. Het is momenteel voor de Commissie onmogelijk in te schatten wat voor impact dit zal hebben op het vlak van verwerking van persoonsgegevens. M.b.t. dit koninklijk besluit wordt dan ook best voorafgaandelijk het advies van de Commissie ingewonnen.

11. Artikel 11.1 van de Uitvoeringsverordening (EU) 2015/1501 van de Europese Commissie van 8 september 2015[4] bepaalt dat bij een **grensoverschrijdende** transactie een minimaal pakket aan persoonsidentificatiegegevens – opgesomd in de bijlage - moet worden meegestuurd. Dit pakket bevat **verplicht**: de huidige familienaam of familienamen, de huidige voornaam of voornamen, de geboortedatum en een unieke identificatiecode, door de lidstaat van verzending vastgesteld volgens de technische specificatie voor grensoverschrijdende identificatie, zodanig dat deze zo lang mogelijk stabiel blijft. Volgende gegevens zijn **optioneel**: voornaam of voornamen en familienaam of familienamen bij geboorte, geboorteplaats, huidig adres en geslacht.

12. De formulering van deze uitvoeringsverordening maakt geen onderscheid tussen een grensoverschrijdende authenticatie ten behoeve van een openbare dienst en deze ten behoeve van de private sector.

13. Vraag is of de Koning in toepassing van artikel 7, f), tweede lid van de verordening 910/2014 als voorwaarde kan bepalen dat een beperkter pakket van persoonsidentificatiegegevens zal worden meegestuurd wanneer de authenticatie aan de hand van het EIM gebeurt ten behoeve van een speler uit de private sector.

14. Indien niet, dan betekent dit concreet dat informatiegegevens van het Rijksregister worden verstrekt (zie artikel 7 van het voorontwerp) aan buitenlandse commerciële ondernemingen. Op basis van de actuele wet van 8 augustus 1983 *tot regeling van een Rijksregister van de natuurlijke personen*,

---

[4] Uitvoeringsverordening (EU) 2015/1501 van de Commissie van 8 september 2015 *betreffende het interoperabiliteitskader bedoeld in artikel 12, lid 8, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt*, genomen ter uitvoering van de artikelen 9 en 12 verordening 910/2014.

komen commerciële ondernemingen – ongeacht of het buitenlandse dan wel Belgische ondernemingen betreft - niet in aanmerking om informatie uit het Rijksregister te verkrijgen of om het Rijksregisternummer te gebruiken.

15. De Commissie maakt van de gelegenheid gebruik om de aandacht te vestigen op de problematiek van de optioneel mee te sturen gegevens. Vooraleer deze worden meegestuurd, zal voorafgaandelijk moeten worden gecontroleerd of het meesturen ervan in het licht van het nagestreefde doeleinde proportioneel is en zo ja, welke van deze gegevens proportioneel zijn (artikel 4, § 1, 3°, WVP). Uit artikel 7 van het voorontwerp blijkt dat de Federale Overheidsdienst Informatie- en Communicatietechnologie (hierna Fedict) zal instaan voor het meesturen ervan. Het is bijgevolg Fedict die erover moet waken dat het proportionaliteitsbeginsel wordt gerespecteerd. De Commissie is van oordeel dat het niet aan Fedict als technisch knooppunt is om te bepalen welke optionele gegevens in een concreet geval proportioneel zijn. De Commissie of het bevoegde sectorale comité zijn beter geplaatst om daarover te beslissen en dit wordt dan ook best in de regelgeving opgenomen. Hoe dan ook is het aangewezen vooraleer tot de effectieve verzending van optionele gegevens over te gaan de betrokkene te informeren zodat hij de mogelijkheid heeft de operatie stop te zetten wanneer hij van oordeel is dat de verstrekking van een of meer optionele gegevens niet ter zake dienend is.

Artikel 6, § 1, voorontwerp

16. Uit artikel 6.1. van de verordening 910/2014 blijkt dat de verplichte wederzijdse erkenning enkel speelt voor de EIM waarvan het betrouwbaarheidsniveau gelijk of hoger is dan het betrouwbaarheidsniveau dat door de openbare dienst als voorwaarde wordt gesteld en voor zover dit niveau substantieel of hoog is. Ingeval van een betrouwbaarheidsniveau "laag" is de erkenning facultatief (artikel 6.2. van de verordening 910/2014).

17. Het is met het oog hierop dat artikel 6, § 1, van het voorontwerp overheden die online diensten aanbieden verplicht om het noodzakelijke betrouwbaarheidsniveau, vereist om toegang te krijgen tot deze diensten, te bepalen. Dit is noodzakelijk om te kunnen vaststellen of de wederzijdse erkenning van EIM van toepassing is en in positief geval, aan de hand van welke EIM toegang moet worden verleend.

18. De overheid (= verantwoordelijke voor de verwerking) die een onlinedienst aanbiedt is het best geplaatst om het vereiste betrouwbaarheidsniveau in te schatten. Zij zal een grondige analyse moeten maken waarbij o.a. rekening wordt gehouden met de hoeveelheid van gegevens die per persoon worden verzameld, aantal personen waarvan gegevens worden verzameld, de aard van de gegevens die worden verzameld (gevoelig of niet), risico op toegang tot /wijziging/vernietiging van de

gegevens door onbevoegden en de schade die daardoor kan worden veroorzaakt, worden alleen leesrechten of ook schrijfrechten verleend, kunnen derden ten behoeve van een derde toegang hebben/handelingen stellen...

Artikel 6, § 2, voorontwerp

19. Het bepalen van het betrouwbaarheidsniveau van de EIM[5] die door Fedict zullen worden aangemeld, is een beslissing met verstrekkende gevolgen voor alle overheidsdiensten die elektronische diensten ter beschikking stellen. Wanneer het betrouwbaarheidsniveau van een EIM als "substantial" of "high" wordt bepaald en aldus wordt aangemeld, zullen de Belgische overheidsdiensten die toegang verlenen op basis van EIM met dergelijke niveau verplicht zijn om de aangemelde buitenlandse EIM van hetzelfde niveau toe te laten, wat voor problemen kan zorgen.

20. Om te vermijden dat Belgische overheden voor een voldongen feit worden gesteld, is de verplichting in hoofde van Fedict om, voorafgaand aan de bepaling van het betrouwbaarheidsniveau en de aanmelding, overleg te plegen met zoveel mogelijk betrokken spelers via het College van voorzitters van de Federale en Programmatorische Overheidsdiensten, het College van afgevaardigd bestuurders van de instellingen van sociale zekerheid en het College van afgevaardigd bestuurders van de federale instellingen van openbaar nut, een goede zet. Het laat Fedict toe om, vooraleer tot aanmelding over te gaan, tot een weloverwogen afweging te komen die rekening houdt met zowel technische als praktische aspecten.

Artikel 7 voorontwerp

21. Paragraaf 1 van dit artikel belast Fedict n.a.v. een grensoverschrijdende identificatie met het verstrekken van de verplichte en optionele persoonsidentificatiegegevens zoals bepaald in de uitvoeringsverordening (EU) 2015/1501. Met het oog hierop verleent artikel 7, §§ 2 en 3 van het voorontwerp Fedict toegang tot de informatiegegevens van het Rijksregister.

22. Er wordt dus afgeweken van de principiële bevoegdheid van het Sectoraal comité van het Rijksregister zoals voorzien door de wet van 8 augustus 1983. De wetgever kan via een rechtsnorm van gelijke rang uitzonderingen voorzien op de procedure opgelegd door de wet van 8 augustus 1983[6].

---

[5] In uitvoeringsverordening (EU) nr. 2015/1502 zijn minimale technische specificaties, normen en procedures vastgelegd aan de hand waarvan het betrouwbaarheidsniveau kan worden bepaald.

[6] Zie in verband met deze problematiek ook randnummers 22 en 23 van het advies van de Commissie nr.15/2006 van 14 juni 2006 *betreffende het ontwerp van koninklijk besluit tot regeling van de medewerking aan de vereniging belast met de registratie van de kilometerstand van voertuigen.*

23. De verplicht mee te sturen identificatiegegevens zijn opgenomen op de chip van de eID. In theorie zouden deze gegevens kunnen worden uitgelezen en vervolgens meegestuurd. Dit is echter geen optie gelet op het feit dat:

- naar alle waarschijnlijkheid ook andere EIM dan de eID zullen worden aangemeld;
- de eID ook op een niet-verbonden manier zal worden gebruikt waardoor het uitlezen van de chip niet mogelijk is.

24. De meest praktische manier om die gegevens mee te sturen, is dus een beroep te doen op de relevante authentieke bron, namelijk het Rijksregister. Fedict zal de verplichte gegevens alleen ophalen uit het Rijksregister. Hij haalt ze niet op voor eigen gebruik maar voor mededeling aan buitenlandse overheids- en/of privé-instanties. Men zou kunnen stellen dat er een oneigenlijke mededeling van informatiegegevens van het Rijksregister wordt georganiseerd ten behoeve van instanties die op basis van de wet van 8 augustus 1983 niet in aanmerking komen om dergelijke mededeling te verkrijgen. In het licht hiervan oordeelt de Commissie dat het raadzaam is om de mededeling van de gegevens uit het Rijksregister aan buitenlandse spelers wettelijk te regelen om iedere discussie te vermijden.

25. Voor wat de verplicht te verstrekken identificatiegegevens betreft, stelt er zich gelet op het bepaalde in de uitvoeringsverordening (EU) 2015/1501, geen probleem qua finaliteit en proportionaliteit. Voor wat de optioneel mee te delen identificatiegegevens betreft, ligt dit enigszins anders. Daar zal geval per geval moeten worden beoordeeld of de verstrekking van de optionele gegevens, rekening houdend met het doeleinde, proportioneel is. In dat geval zal voorafgaandelijk het advies van het bevoegde sectorale comité of toezichthoudende autoriteit moeten worden ingewonnen. N.a.v. de verordening (EU) 2016/679 van het Europees Parlement en de Raad van 26 april 2016 *betreffende de bescherming van de natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG*, kunnen de Commissie en haar sectorale comités worden hervormd. De voorgestelde formulering zou een onafhankelijke toetsing van de proportionaliteit moeten waarborgen, ongeacht hoe die hervorming uitvalt. In dit verband verwijst de Commissie naar haar opmerking in randnummer 15.

26. Wat met het oog op transparantie vanwege Fedict mag worden verwacht, is dat hij vooraleer de identificatie- en authenticatie procedure te starten, aan de betrokkene meldt welke minimale identificatiegegevens ingevolge de door uitvoeringsverordening (EU) 2015/1501 opgelegde verplichting moeten worden meegestuurd en dat deze gegevens daartoe uit het Rijksregister zullen worden opgehaald. Vervolgens moet de betrokkene die niet wenst dat die mededeling gebeurt, de mogelijkheid hebben om de procedure niet op te starten.

27. Vermits deze paragraaf een uitzondering vormt op de bepalingen van de wet van 8 augustus 1983, is het aangewezen om terminologisch bij die wet aan te sluiten en de passage:

> *"... heeft de federale overheidsdienst Informatie- en Communicatietechnologie het recht om de nodige gegevens op te halen in het Rijksregister".*

te vervangen door

> *" ... wordt de federale overheidsdienst Informatie- en Communicatietechnologie gemachtigd om de in § 1 bedoelde gegevens op te halen in het Rijksregister.*

28. Door "*de nodige gegevens*" te vervangen door de "*in § 1 bedoelde gegevens*", wordt benadrukt dat de toegang beperkt is tot de gegevens die deel uitmaken van het minimale gegevenspakket zoals vastgesteld in de bijlage van de uitvoeringsverordening (EU) 2015/1501.

29. Paragraaf 3 anticipeert op een eventuele toekomstige uitbreiding van de optionele gegevens die ingevolge de verordening 910/2014 of haar uitvoeringsverordening zou mogelijk worden, door daarvoor reeds door deze wet in een toegang tot het Rijksregister te voorzien. Net zoals dat voor paragraaf 2 het geval was, wordt de formulering ervan best in overeenstemming gebracht met de terminologie gehanteerd in de wet van 8 augustus 1983. Er wordt dan ook voorgesteld om de tekst van deze paragraaf als volgt te vervangen:

> *"Om te voldoen aan een verplichting van de verordening 910/2014 of één van haar uitvoeringshandelingen die de uitwisseling van bijkomende persoonsidentificatiegegevens mogelijk maakt, wordt de Federale Overheidsdienst Informatie- en Communicatietechnologie gemachtigd, na advies van het bevoegde sectorale comité of de toezichthoudende autoriteit zoals bedoeld in hoofdstuk VI van de verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG, om de overeenkomstige gegevens op te halen in het Rijksregister".*

Artikel 8 voorontwerp

30. Dit artikel organiseert het toezicht en de controle op de aangemelde stelsels van elektronische identificatie.

31. De Commissie stelt vooreerst vast dat het voorontwerp niet aangeeft welke instantie de rol van toezichthoudend orgaan zal opnemen. De steller van het voorontwerp vermelde hierover in zijn bijkomende toelichting van 22/08/2016 het volgende: *"Wij zijn er ons van bewust dat deze bevoegdheid zo snel mogelijk aan een neutraal orgaan met de nodige expertise moet worden toegewezen en zullen hier dan ook een prioriteit van maken."* De Commissie onderschrijft dit standpunt, en zij is van oordeel dat de aanduiding van dit orgaan best in het voorontwerp gebeurt. In de mate dat Fedict medeverantwoordelijk is voor een EIM, namelijk de EID, lijkt het niet aangewezen dat het de rol van toezichthoudend orgaan op zich neemt.

32. Artikel 10 van de verordening 910/2014 bepaalt dat indien de integriteit van delen van het stelsel voor elektronische identificatie en authenticatie geschonden is, de aanmeldende lidstaat deze onverwijld moet opschorten of intrekken en de Europese Commissie en de andere lidstaten daarvan informeren. Artikel, 8, § 5, van het voorontwerp bepaalt dat het toezichthoudend orgaan een aangemeld systeem voor elektronische identificatie kan intrekken of opschorten indien de integriteit ervan geschonden is. Het is niet duidelijk wie zal instaan voor de melding aan de Europese Commissie en de andere lidstaten. Om ieder misverstand te vermijden moet worden gepreciseerd wie deze melding zal doen, gelet op het belang van deze melding en de eventuele nefaste gevolgen op het vlak van gegevensverwerking indien deze niet gebeurt.

33. Artikel 8, §§ 3 en 4, van het voorontwerp regelen de situatie waarin het toezichthoudend orgaan vaststelt dat de uitgever van een EIM of de partij die de authenticatieprocedure uitvoert de eisen van de verordening 910/2014 niet respecteert. Het gaat dus kennelijk om inbreuken die niet direct een impact hebben op de integriteit van het proces. In zoverre dit betekent dat er geen risico bestaat dat de persoonsgegevens die in het kader van het proces worden verwerkt in gevaar komen (verlies, ongeoorloofde wijziging, ongeoorloofde toegang, diefstal), is het niet problematisch dat de betrokken instantie de tijd krijgt om zich opnieuw te conformeren. De Commissie oordeelt dat vanaf het ogenblik dat de inbreuk de verwerkte persoonsgegevens in gevaar brengt, de mogelijkheid moet worden voorzien dat het stelsel onmiddellijk kan worden opgeschort of ingetrokken, in afwachting dat de betrokken instantie zich in regel stelt. In het licht van artikel 16 WVP kan moeilijk worden verantwoord dat men een systeem dat niet langer voldoet aan de gestelde eisen, verder laat functioneren.

B. ELEKTRONISCHE IDENTIFICATIE VOOR BELGISCHE OVERHEIDSTOEPASSINGEN.

Artikel 11, § 3, voorontwerp

34. In deze paragraaf wordt weerom afgeweken van de bevoegdheid van het Sectoraal comité van het Rijksregister zoals geregeld door de wet van 8 augustus 1983. Er wordt een wettelijke machtiging verleend aan Fedict om het Rijksregisternummer te gebruiken. Er wordt echter niet gemotiveerd waarom deze wettelijke uitzondering noodzakelijk is. In de toelichting bij deze bepaling wordt trouwens gemeld dat Fedict reeds door het Sectoraal comité van het Rijksregister gemachtigd werd om het Rijksregisternummer voor authenticatiedoeleinden te gebruiken. Deze paragraaf is dus overbodig en dient te worden geschrapt.

Artikel 12 voorontwerp

35. Dit artikel biedt de mogelijkheid toegang te verkrijgen tot digitale overheidstoepassingen op basis van een dienst voor elektronische identificatie, geleverd door spelers die geen openbare instanties zijn. Tegen dit beginsel *an sich* heeft de Commissie geen bezwaar[7]. Ten gronde kan de Commissie zich momenteel niet uitspreken vermits de procedure, de voorwaarden en de gevolgen van de erkenning door de Koning worden bepaald. Er wordt voorzien dat m.b.t. het te nemen koninklijk besluit het advies wordt ingewonnen van het bevoegde sectoraal comité of de toezichthoudende autoriteit. Inzake is het aangewezen dat het advies van de toezichthoudende autoriteit, normaliter de Commissie dus, wordt ingewonnen en niet zozeer dat van een sectoraal comité. Het is positief dat, naar analogie met artikel 6, § 2, van het voorontwerp, een voorafgaande raadpleging van de betrokken spelers wordt opgelegd (zie ook randnummer 21).

36. Niettegenstaande artikel 12, § 2, van het voorontwerp de Koning belast met het bepalen van de procedure, de voorwaarden en de gevolgen van de erkenning, worden er enkele aspecten op ondubbelzinnige wijze in artikel 12, § 5, van het voorontwerp geregeld. In de eerste plaats wordt uitdrukkelijk bepaald dat de aanbieder van een erkende dienst voor elektronische identificatie door de wet gemachtigd wordt om het Rijksregisternummer te gebruiken. Uit de memorie blijkt dat dit gebruik beperkt is tot het toegangs- en gebruikersbeheer via de Federale Authentication Service (FAS) voor overheidsdiensten. Verder wordt in de memorie gesignaleerd dat indien een erkende aanbieder het Rijksregisternummer buiten het kader waarvoor hij erkend werd, wenst te gebruiken, hij daartoe bij het bevoegde sectorale comité een machtiging zal moeten aanvragen. Duidelijkheidshalve en om

---

[7] In dezelfde lijn: de Commissie adviseerde gunstig in haar advies 20/2014 van 19 maart 2014 *betreffende het ontwerp van Koninklijk besluit tot vaststelling van de voorwaarden, de procedure en de gevolgen van de erkenning van aanmeldingsdiensten voor digitale overheidstoepassingen die gebruik maken van niet-verbonden aanmeldingsmiddelen*, dat de inschakeling mogelijk maakt van aanmeldingsdiensten uit de private sector.

misverstanden te vermijden wordt de beperking van het gebruik van het Rijksregisternummer best in de wet opgenomen.

37. De erkende aanbieders bieden doorgaans nog andere diensten aan waardoor het risico reëel is dat zij de persoonsgegevens die zij verzamelden met het oog op het doeleinde waarvoor zij erkend zijn, voor andere commerciële doeleinden zullen gebruiken. In de artikelsgewijze bespreking wordt opgemerkt dat er garanties zullen gevraagd worden om dit te beletten. Deze zullen deel uitmaken van de door de Koning vast te stellen voorwaarden voor erkenning. De Commissie neemt hier akte van en zij gaat er van uit dat voornoemd toekomstig uitvoeringsbesluit haar nog in een later stadium voor advies zal voorgelegd worden. Tegelijk dringt zij er op aan om reeds in het voorontwerp het principe op te nemen dat de persoonsgegevens die worden verzameld in het kader van de elektronische identificatie, niet voor andere doeleinden mogen worden gebruikt.

38. Verder verleent artikel 12, § 5, van het voorontwerp een wettelijke machtiging aan de erkende diensten voor elektronische identificatie om het Rijksregisternummer te gebruiken. Er wordt echter niet gemotiveerd waarom deze wettelijke uitzondering op de regeling opgenomen in de wet van 8 augustus 1983 noodzakelijk is. In het artikel zelf wordt bepaald dat de aanbieder van een erkende dienst voor elektronische identificatie moet worden beschouwd als een onderaannemer van de erkennende overheid, *in casu* Fedict, in de zin van artikel 5, eerste lid, 3°, van de wet van 8 augustus 1983. Deze specificering volstaat om dergelijke erkende aanbieder op basis van de bepalingen van de wet van 8 augustus 1983 te machtigen. Er is bijgevolg geen objectieve redenen om voor deze doelgroep een uitzondering op de wet van 8 augustus 1983 op te nemen. De tekst van deze paragraaf wordt bijgevolg best beperkt tot :

> *"De aanbieder van een erkende dienst voor elektronische identificatie wordt voor de toepassing van dit artikel beschouwd als een onderaannemer van de erkennende overheid in de zin van artikel 5, eerste lid, 3°, van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen".*

De Commissie vestigt er volledigheidshalve de aandacht op dat indien een aanbieder van een erkende dienst voor elektronische identificatie met het oog deze dienst gegevens wenst te verifiëren in het Rijksregister, hij daartoe een machtiging zal moeten aanvragen bij het bevoegde sectoraal comité.

Artikel 13 voorontwerp

39. Het eerste lid van dit artikel draagt de zorg voor het EIM op aan de houder ervan (exclusieve controle, beschermen tegen verlies, diefstal). In de artikelsgewijze bespreking wordt gepreciseerd dat exclusieve controle onder meer inhoudt dat paswoorden strikt confidentieel worden

gehouden. De Commissie stelt vast dat het voor een aantal burgers onmogelijk is om bijvoorbeeld hun paswoorden strikt confidentieel te houden.

40. Steeds meer diensten zijn uitsluitend digitaal toegankelijk, terwijl een deel van de bevolking zich hieraan niet heeft kunnen aanpassen. Wanneer zo iemand op bepaalde diensten beroep wenst te doen, heeft hij vaak geen andere keuze dan bijvoorbeeld zijn eID te overhandigen aan een derde en deze laatste eveneens zijn pincode te verschaffen. De derde waarop hij beroep doet, zal wellicht iemand zijn die hij als integer inschat en die dus geen misbruik zal maken van dit instrument. Quid als deze derde dit toch doet. Is de houder van het EIM dan in de zin van dit artikel van het voorontwerp tekortgeschoten?

41. Artikel 13, tweede lid, van het voorontwerp bepaalt dat een EIM dat niet meer geldig is of ingetrokken is, niet meer door de houder mag worden gebruikt. Uit de bijkomende toelichting van de steller van het voorontwerp van 22 augustus 2016, blijkt dat het niet ongewoon is om de houder van een EIM op die manier te responsabiliseren. Uit de tekst blijkt dat alleen de houder die ter kwader trouw is (gebruikt zijn EIM goed wetende deze vervallen of ingetrokken is) wordt geviseerd. De Commissie neemt hier akte van en vestigt er volledigheidshalve de aandacht op dat een dergelijke responsabilisering van de houder, evident geen afbreuk doet aan de verplichtingen en verantwoordelijkheden van de andere actoren (zoals de aanbieder van het EIM).

OM DEZE REDENEN,
de Commissie

verleent gunstig advies voor zover rekening wordt gehouden met de opmerkingen geformuleerd in de punten 5, 13-15, 25-29, 31, 32, 34, 36-38 en 41.

De Wnd. Administrateur,

An Machtens

De Voorzitter,

Willem Debeuckelaere

Avis n° 48/2016 du 21 septembre 2016

Objet : avis concernant l'avant-projet de loi relative à l'identification électronique (CO-A-2016-032)

La Commission de la protection de la vie privée (ci-après "la Commission") ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après "la LVP"), en particulier l'article 29 ;

Vu la demande d'avis de Monsieur Jan DEPREST, Président du Service public fédéral ICT, reçue le 13/05/2016 ;

Vu les textes adaptés de l'avant-projet, reçus le 25/05/2016, le 13/07/2016 et le 14/09/2016, et vu les explications complémentaires reçues le 22/08/2016 ;

Vu le rapport de Monsieur Ivan VANDERMEERSCH ;

Émet, le 21 septembre 2016, l'avis suivant :

REMARQUE PRÉALABLE

La Commission attire l'attention sur le fait qu'une nouvelle réglementation européenne relative à la protection des données à caractère personnel a été promulguée récemment : le Règlement général relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et la Directive Police et Justice. Ces textes ont été publiés au journal officiel de l'Union européenne le 4 mai 2016[1].

Le Règlement, couramment appelé GDPR (General Data Protection Regulation), est entré en vigueur vingt jours après sa publication, soit le 24 mai 2016, et est automatiquement applicable deux ans plus tard, soit le 25 mai 2018. La Directive Police et Justice doit être transposée dans la législation nationale au plus tard le 6 mai 2018.

Pour le Règlement, cela signifie que depuis le 24 mai 2016, pendant le délai d'exécution de deux ans, les États membres ont d'une part une obligation positive de prendre toutes les dispositions d'exécution nécessaires, et d'autre part aussi une obligation négative, appelée "devoir d'abstention". Cette dernière obligation implique l'interdiction de promulguer une législation nationale qui compromettrait gravement le résultat visé par le Règlement. Des principes similaires s'appliquent également pour la Directive.

Il est dès lors recommandé d'anticiper éventuellement dès à présent ces textes. Et c'est en premier lieu au(x) demandeur(s) de l'avis qu'il incombe d'en tenir compte dans ses (leurs) propositions ou projets. Dans le présent avis, la Commission a d'ores et déjà veillé, dans la mesure du possible et sous réserve d'éventuels points de vue complémentaires ultérieurs, au respect de l'obligation négative précitée.

I. CONTEXTE

1. L'avant-projet de loi relative à l'identification électronique, ci-après "l'avant-projet", comprend 2 volets. Le premier volet comporte un certain nombre de mesures qui sont nécessaires pour appliquer

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* (règlement général sur la protection des données)
Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données et abrogeant la décision-cadre 2008/977/JAI du Conseil*
http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC
)

le chapitre II du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 *sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE* (ci-après "le règlement 910/2014").

2. Le deuxième volet étaie juridiquement l'identification électronique pour les applications publiques en ce qui concerne la Belgique.

3. L'identification électronique se fait via des systèmes numériques et va de pair avec le traitement automatisé de données à caractère personnel. Les dispositions de la LVP sont donc applicables. L'analyse se limite aux articles qui donnent lieu au traitement de données à caractère personnel.

II. EXAMEN QUANT AU FOND

A. APPLICATION DU CHAPITRE II DU RÈGLEMENT 910/2014

Généralités

4. Afin de pouvoir utiliser des services électroniques, une identification et une authentification électroniques sont généralement requises. Celles-ci constituent une pierre d'achoppement pour l'utilisation transfrontalière de services électroniques car un citoyen ne peut pas utiliser son moyen d'identification électronique (ci-après MIE) parce que son système national d'identification et d'authentification électroniques n'est pas reconnu dans les autres États membres. Le règlement 910/2014 entend lever cet obstacle, en tout cas en ce qui concerne l'identification et l'authentification vis-à-vis du secteur public. Le chapitre II définit la manière dont cela s'effectuera, à savoir en élaborant un système de reconnaissance mutuelle obligatoire de MIE[1]. Les MIE étrangers ainsi reconnus doivent pouvoir être utilisés en Belgique sans entraves. Des règlements d'exécution établissent des règles plus détaillées en vue de la mise en application de ce système de reconnaissance mutuelle. À titre d'exemple :

a) Le règlement d'exécution (UE) n° 2015/1501 traite de ce qu'on appelle le "cadre d'interopérabilité" (qui a pour but d'assurer l'interopérabilité des schémas d'identification électronique notifiés par les États membres à la Commission européenne). Ce règlement

[1] L'article 7 du règlement 910/2014 contient les conditions qu'un schéma d'identification électronique doit remplir pour être éligible pour la notification à la Commission européenne. Au plus tard un an après la publication par la Commission européenne des schémas d'identification électronique qui ont été notifiés, ceux-ci doivent être reconnus (articles 6.1 et 9.2 du règlement 910/2014).

d'exécution définit également des règles relatives à la sécurité des données et, dans ce cadre, fait reposer une importante responsabilité auprès des dits "nœuds"[2].

b) Le règlement d'exécution (UE) n° 2015/1502 fixe des spécifications techniques, des normes et des procédures minimales permettant de définir le niveau de garantie d'un MIE. Ce règlement d'exécution contient également des règles en matière de "demande et enregistrement", de "preuve et vérification d'identité", de "délivrance et activation".

5. La Commission constate en outre que dans le cadre d'une identification et d'une authentification transfrontalières, ce n'est pas le numéro de Registre national qui est communiqué mais le STORK-ID (constitué sur la base du numéro de Registre national). Selon les informations complémentaires de l'auteur de l'avant-projet, reçues par la Commission le 22 août 2016, la Belgique n'est pas un cas isolé à ce niveau et chaque pays européen travaille avec un numéro transnational unique afin d'identifier ses citoyens dans un contexte transnational[3]. Afin d'expliquer la distinction entre l'utilisation d'un numéro unique dans l'identification transfrontalière et l'identification nationale, il serait préférable d'intégrer dans l'exposé des motifs les informations complémentaires que l'auteur de l'avant-projet a transmises à cet égard à la Commission le 22 août 2016.

Article 5, § 1er de l'avant-projet

6. En fait, il s'agit d'une intervention de légistique purement formelle qui met en conformité avec le règlement 910/2014 toute réglementation belge prescrivant l'utilisation de MIE belges pour accéder à un service électronique, sans que des dispositions individuelles de la réglementation belge ne doivent être adaptées. En vertu de cette disposition, les MIE étrangers reconnus présentant le même niveau de garantie que le MIE belge devront être autorisés.

7. Vu les dispositions du règlement 910/2014 d'une part et le fait que l'équivalence se limite aux MIE présentant le même niveau de garantie que celui requis par la réglementation belge d'autre part, cela ne pose pas de problèmes spécifiques du point de vue de la LVP. Par pur souci d'exhaustivité, la Commission attire l'attention sur le fait qu'il faut veiller à ce que la sécurité de la chaîne par le biais de laquelle le processus d'identification et d'authentification se déroule à l'aide du MIE étranger soit assurée et à ce qu'une piste d'audit complète soit disponible. Cela requiert que tous les maillons de la

---

[2] En Belgique, Fedict assume le rôle de "nœud" (article 10 de l'avant-projet).

[3] À la question de savoir si un tel système dans notre pays ne conduit pas à un traitement inégal car les Belges sont obligés "en interne" de fournir leur numéro de Registre national alors que ce n'est pas le cas lors d'une identification transfrontalière, l'auteur répond ce qui suit : "*Toute personne reprise dans le Registre national est identifiée de manière unique par les instances belges habilitées à l'aide du numéro de Registre national. Ces mêmes personnes sont identifiées dans un contexte transnational européen à l'aide d'un numéro dérivé. Il s'agit donc des mêmes personnes qui sont identifiées d'une autre manière dans un autre contexte. (...) Cette méthode s'applique à toute personne de la même façon (en Belgique, le numéro de Registre national, en dehors de la Belgique et au sein de l'UE, d'une autre manière (...)*" [traduction libre réalisée par le Secrétariat de la Commission, en l'absence de traduction officielle].

chaîne puissent être identifiés et que des accords et/ou des garanties entre tous les maillons de la chaîne soient convenu(e)s (circles of trust ou cercles de confiance).

Article 5, § 2 de l'avant-projet

8. Le considérant 17 - qui se rapporte à l'article 7, f), deuxième alinéa du règlement 910/2014 - incite les États membres à encourager le secteur privé à utiliser des MIE notifiés.

9. L'article 5, § 2 de l'avant-projet recourt à la possibilité offerte par l'article 7, f), deuxième alinéa du règlement 910/2014, à savoir soumettre l'utilisation par le secteur privé de MIE notifiés à des conditions. Le Roi est chargé de définir ces conditions.

10. Actuellement, il est impossible à la Commission d'évaluer l'impact que cela aura au niveau du traitement de données à caractère personnel. Il serait dès lors préférable de recueillir préalablement l'avis de la Commission concernant cet arrêté royal.

11. L'article 11.1 du Règlement d'exécution (UE) 2015/1501 de la Commission européenne du 8 septembre 2015[4] dispose que dans le cadre d'une transaction **transfrontalière**, un ensemble minimal de données d'identification personnelle - énumérées dans l'annexe - doit être transmis. Cet ensemble comporte **obligatoirement** : le(s) nom(s) de famille actuel(s), le(s) prénom(s) actuel(s), la date de naissance et l'identifiant unique créé par l'État membre expéditeur conformément aux spécifications techniques aux fins de l'identification transfrontalière et qui soit aussi persistant que possible dans le temps. Les données suivantes sont **optionnelles** : prénom(s) et nom(s) de famille à la naissance, lieu de naissance, adresse actuelle et sexe.

12. La formulation de ce règlement d'exécution ne fait pas de distinction entre une authentification transfrontalière au profit d'un service public et celle au profit du secteur privé.

13. La question se pose de savoir si en application de l'article 7, f), deuxième alinéa du règlement 910/2014, le Roi peut poser comme condition qu'un ensemble plus limité de données d'identification personnelle soit transmis lorsque l'authentification se fait à l'aide du MIE au profit d'un acteur du secteur privé.

14. Si tel n'est pas le cas, cela signifie concrètement que des informations du Registre national sont fournies (voir l'article 7 de l'avant-projet) à des entreprises commerciales étrangères. En vertu

[4] Règlement d'exécution (UE) 2015/1501 de la Commission du 8 septembre 2015 *sur le cadre d'interopérabilité visé à l'article 12, paragraphe 8, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur*, adopté en exécution des articles 9 et 12 du règlement 910/2014.

de l'actuelle loi du 8 août 1983 *organisant un registre national des personnes physiques*, les entreprises commerciales – qu'il s'agisse d'entreprises étrangères ou belges – n'entrent pas en ligne de compte pour obtenir des informations du Registre national ou utiliser le numéro de Registre national.

15. La Commission profite de l'occasion pour attirer l'attention sur la problématique des données qui peuvent être transmises de manière optionnelle. Avant que celles-ci soient transférées, il faudra préalablement contrôler si leur envoi est proportionnel à la lumière de la finalité poursuivie et si oui, quelles données parmi celles-ci sont proportionnelles (article 4, § 1, 3° de la LVP). Il ressort de l'article 7 de l'avant-projet que le Service public fédéral Technologie de l'Information et de la Communication (ci-après Fedict) se chargera de l'envoi. Dès lors, c'est Fedict qui doit veiller au respect du principe de proportionnalité. La Commission estime qu'il n'appartient pas à Fedict, en tant que nœud technique, de déterminer quelles données optionnelles sont proportionnelles dans un cas concret. La Commission ou le comité sectoriel compétent sont mieux placés pour en décider et il serait dès lors souhaitable de reprendre cette information dans la réglementation. Il est quoi qu'il en soit recommandé d'informer la personne concernée avant de procéder à l'envoi effectif de données optionnelles de manière à ce qu'elle ait la possibilité de mettre un terme à l'opération lorsqu'elle juge que la communication d'une ou de plusieurs données optionnelles n'est pas pertinente.

Article 6, § 1er de l'avant-projet

16. Il ressort de l'article 6.1. du règlement 910/2014 que la reconnaissance mutuelle obligatoire ne joue que pour les MIE dont le niveau de garantie est égal ou supérieur à celui requis par l'organisme du secteur public concerné et pour autant que ce niveau soit substantiel ou élevé. En cas de niveau de garantie "faible", la reconnaissance est facultative (article 6.2. du règlement 910/2014).

17. C'est à cette fin que l'article 6, § 1er de l'avant-projet oblige les autorités qui proposent des services en ligne à déterminer le niveau de garantie nécessaire, requis pour accéder à ces services. C'est essentiel pour pouvoir établir si la reconnaissance mutuelle de MIE est d'application et, dans l'affirmative, à l'aide de quel MIE un accès doit être accordé.

18. L'autorité (= le responsable du traitement) qui propose un service en ligne est la mieux placée pour évaluer le niveau de garantie requis. Elle devra réaliser une analyse approfondie qui tiendra notamment compte de la quantité de données qui sont collectées par personne, du nombre de personnes dont des données sont collectées, de la nature des données qui sont collectées (sensibles ou pas), du risque d'accès aux données, du risque de modification/de destruction des données par des personnes non habilitées et des dommages que cela peut engendrer, du fait que seuls des droits de lecture sont accordés ou également des droits d'écriture, du fait que des tiers peuvent obtenir un accès/effectuer des opérations au profit d'un tiers, ...

Article 6, § 2 de l'avant-projet

19. La définition du niveau de garantie des MIE[5] qui seront notifiés par Fedict est une décision lourde de conséquences pour tous les services publics qui mettent à disposition des services électroniques. Lorsque le niveau de garantie d'un MIE est défini comme "substantial" ou "high" et donc notifié comme tel, les services publics belges qui accordent un accès sur la base d'un MIE présentant un tel niveau seront obligés d'autoriser les MIE étrangers notifiés du même niveau, ce qui peut occasionner des problèmes.

20. Afin d'éviter que des autorités belges ne soient mises devant le fait accompli, l'obligation, dans le chef de Fedict, de consulter le plus grand nombre possible d'acteurs concernés, via le Collège des présidents des services publics fédéraux et des services publics de programmation, le Collège des administrateurs délégués des institutions de la sécurité sociale et le Collège des administrateurs délégués des organismes d'intérêt public fédéraux, avant la définition du niveau de garantie et la notification, est une bonne chose. Cela permet à Fedict, avant de procéder à la notification, de réaliser une pondération réfléchie qui tient compte aussi bien des aspects techniques que pratiques.

Article 7 de l'avant-projet

21. Le paragraphe 1er de cet article charge Fedict, lors d'une identification transfrontalière, de fournir les données d'identification personnelle obligatoires et optionnelles telles que définies dans le règlement d'exécution (UE) 2015/1501. À cet effet, les §§ 2 et 3 de l'article 7 de l'avant-projet accordent à Fedict un accès aux informations du Registre national.

22. Il est donc dérogé à la compétence de principe du Comité sectoriel du Registre national telle que prévue par la loi du 8 août 1983. Le législateur peut, via une norme juridique de rang égal, prévoir des exceptions à la procédure imposée par la loi du 8 août 1983[6].

23. Les données d'identification qui doivent obligatoirement être envoyées sont reprises sur la puce de la carte d'identité électronique (eID). En théorie, ces données pourraient être lues et ensuite transmises. Ce n'est toutefois pas une option étant donné le fait que :

- selon toute probabilité, d'autres MIE que l'eID seront également notifiés ;

---

[5] Le règlement d'exécution (UE) n° 2015/1502 fixe des spécifications techniques, des normes et des procédures minimales permettant de définir le niveau de garantie.

[6] Concernant cette problématique, voir également les points 22 et 23 de l'avis de la Commission n° 15/2006 du 14 juin 2006 *relatif au projet d'arrêté royal réglant la collaboration à l'association chargée de l'enregistrement du kilométrage des véhicules.*

- l'eID sera également utilisée d'une manière non-connectée, rendant la lecture de la puce impossible.

24. La manière la plus pratique de transmettre ces données est donc de recourir à la source authentique pertinente, à savoir le Registre national. Fedict extraira juste les données obligatoires du Registre national. Il ne les extrait pas pour son propre usage mais pour une communication à des instances publiques et/ou privées étrangères. On pourrait affirmer qu'une communication impropre d'informations du Registre national est organisée au profit d'instances qui, sur la base de la loi du 8 août 1983, n'entrent pas en ligne de compte pour obtenir une telle communication. À la lumière de cet élément, la Commission estime qu'il convient de régir la communication des données du Registre national à des acteurs étrangers afin d'éviter toute discussion.

25. En ce qui concerne les données d'identification qu'il faut obligatoirement fournir, vu ce que prévoit le règlement d'exécution (UE) 2015/1501, aucun problème ne se pose en matière de finalité et de proportionnalité. Quant aux données d'identification qui peuvent être communiquées de manière optionnelle, la situation est quelque peu différente. Il faudra évaluer au cas par cas si la communication des données optionnelles est proportionnelle, compte tenu de la finalité. Dans ce cas, l'avis du comité sectoriel compétent ou de l'autorité de contrôle devra être préalablement recueilli. En vertu du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE*, la Commission et ses comités sectoriels peuvent faire l'objet d'une réforme. La formulation proposée devrait garantir un contrôle indépendant de la proportionnalité, quel que soit le résultat de cette réforme. À cet égard, la Commission renvoie à sa remarque émise au point 15.

26. Ce que l'on peut attendre de Fedict en vue de la transparence, c'est qu'avant de lancer la procédure d'identification et d'authentification, il signale à la personne concernée quelles données d'identification minimales doivent être envoyées en vertu de l'obligation imposée par le règlement d'exécution (UE) 2015/1501 et que ces données seront à cet effet extraites du Registre national. La personne concernée qui ne souhaite pas que cette communication ait lieu doit ensuite avoir la possibilité de ne pas lancer la procédure.

27. Étant donné que ce paragraphe constitue une exception aux dispositions de la loi du 8 août 1983, il est recommandé d'utiliser la même terminologie que dans cette loi et de remplacer le passage :

> *"(...) le service public fédéral Technologie de l'Information et de la Communication a le droit d'obtenir les données nécessaires du Registre national"*

par :

> *"(...) le service public fédéral Technologie de l'Information et de la Communication est autorisé à collecter les données visées au § 1er dans le Registre national".*

28. En remplaçant "*les données nécessaires*" par "*les données visées au § 1er*", on insiste sur le fait que l'accès est limité aux données qui font partie de l'ensemble minimal de données tel que défini dans l'annexe du règlement d'exécution (UE) 2015/1501.

29. Le paragraphe 3 anticipe une éventuelle extension future des données optionnelles qui deviendrait possible en vertu du règlement 910/2014 ou de son règlement d'exécution en prévoyant déjà à cet effet par le biais de la présente loi un accès au Registre national. Tout comme c'était le cas pour le paragraphe 2, il est préférable d'harmoniser la formulation avec la terminologie utilisée dans la loi du 8 août 1983. Il est dès lors proposé de remplacer le texte de ce paragraphe comme suit :

> *"Pour satisfaire à une obligation du règlement 910/2014 ou à l'un de ses actes d'exécution qui permet l'échange de données d'identification personnelle supplémentaires, le service public fédéral Technologie de l'Information et de la Communication est autorisé à collecter les données correspondantes dans le Registre national, après avis du comité sectoriel compétent ou de l'autorité de contrôle telle que visée au chapitre VI du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE."*

Article 8 de l'avant-projet

30. Cet article organise la surveillance et le contrôle des schémas d'identification électronique notifiés.

31. La Commission constate tout d'abord que l'avant-projet n'indique pas quelle instance assurera le rôle d'organe de contrôle. À cet égard, l'auteur de l'avant-projet a précisé ce qui suit dans ses explications complémentaires du 22/08/2016 : "*Nous sommes conscients du fait que cette compétence doit être attribuée au plus vite à un organe neutre doté de l'expertise nécessaire et nous en ferons dès lors une priorité.*" [traduction libre réalisée par le Secrétariat de la Commission, en l'absence de traduction officielle]. La Commission adhère à ce point de vue et estime qu'il est préférable de régler la désignation de cet organe dans l'avant-projet. Dans la mesure où Fedict est coresponsable d'un MIE, à savoir l'eID, il ne semble pas indiqué qu'il assume le rôle d'organe de contrôle.

32. L'article 10 du règlement 910/2014 dispose qu'en cas d'altération partielle du schéma d'identification ou d'authentification électronique, l'État membre notifiant doit suspendre ou révoquer immédiatement l'identification et en informer la Commission européenne et les autres États membres. L'article 8, § 5 de l'avant-projet prévoit que l'organe de contrôle peut révoquer ou suspendre un schéma d'identification électronique notifié en cas d'altération de celui-ci. On ne sait pas clairement qui se chargera de la notification à la Commission européenne et aux autres États membres. Afin d'éviter tout malentendu, il faut préciser qui effectuera cette notification, vu l'importance de celle-ci et les éventuelles conséquences négatives au niveau du traitement des données si cette notification n'a pas lieu.

33. Les §§ 3 et 4 de l'article 8 de l'avant-projet régissent la situation dans laquelle l'organe de contrôle constate que l'émetteur d'un MIE ou la partie qui exécute la procédure d'authentification ne respecte pas les exigences du règlement 910/2014. Il s'agit donc manifestement de violations qui n'ont pas directement un impact sur l'intégrité du processus. Dans la mesure où cela signifie qu'il n'y a pas de risque que les données à caractère personnel traitées dans le cadre du processus soient compromises (perte, modification non autorisée, accès non autorisé, vol), il n'est pas problématique que l'instance concernée ait le temps de se conformer à nouveau aux exigences du règlement 910/2014. La Commission estime que dès le moment où la violation compromet les données à caractère personnel traitées, il faut prévoir la possibilité de suspendre ou de révoquer le schéma immédiatement, en attendant que l'instance concernée se mette en règle. À la lumière de l'article 16 de la LVP, on peut difficilement justifier que l'on laisse fonctionner un système qui ne remplit plus les exigences posées.

B. IDENTIFICATION ÉLECTRONIQUE POUR APPLICATIONS PUBLIQUES BELGES

Article 11, § 3 de l'avant-projet

34. Ce paragraphe déroge à nouveau à la compétence du Comité sectoriel du Registre national telle que régie par la loi du 8 août 1983. Une autorisation légale est accordée à Fedict pour utiliser le numéro de Registre national. Toutefois, la nécessité de cette exception légale n'est pas motivée. L'exposé des motifs relatif à cette disposition mentionne d'ailleurs que Fedict a déjà été autorisé par le Comité sectoriel du Registre national à utiliser le numéro de Registre national à des fins d'authentification. Ce paragraphe est donc superflu et doit être supprimé.

Article 12 de l'avant-projet

35. Cet article offre la possibilité d'accéder à des applications publiques numériques sur la base d'un service d'identification électronique, fourni par des acteurs qui ne sont pas des instances publiques. La Commission n'a aucune objection à ce principe en soi[7]. Quant au fond, la Commission ne peut actuellement pas se prononcer étant donné que la procédure, les conditions et les conséquences de l'agrément sont déterminées par le Roi. Il est prévu que l'avis du comité sectoriel compétent ou de l'autorité de contrôle soit demandé concernant l'arrêté royal qui doit être pris. En la matière, il est recommandé que l'avis de l'autorité de contrôle, normalement la Commission donc, soit recueilli plutôt que celui d'un comité sectoriel. Il est positif que, par analogie avec l'article 6, § 2 de l'avant-projet, une consultation préalable des acteurs concernés soit imposée (voir également le point 21).

36. Bien que le § 2 de l'article 12 de l'avant-projet charge le Roi de déterminer la procédure, les conditions et les conséquences relatives à l'agrément, certains aspects sont régis de manière univoque au § 5 de l'article 12. Tout d'abord, il est explicitement précisé que le fournisseur d'un service d'identification électronique agréé est autorisé par la loi à utiliser le numéro de Registre national. Il ressort de l'exposé des motifs que cette utilisation est limitée à la gestion des utilisateurs et des accès via le Federal Authentication Service (FAS, Service fédéral d'authentification) pour les services publics. En outre, l'exposé des motifs signale que si un fournisseur agréé souhaite utiliser le numéro de Registre national en dehors du cadre pour lequel il a été agréé, il devra à cet effet demander une autorisation auprès du comité sectoriel compétent. Par souci de clarté et afin d'éviter les malentendus, il conviendrait de reprendre cette limitation de l'utilisation du numéro de Registre national dans la loi.

37. Les fournisseurs agréés proposent généralement encore d'autres services, rendant réel le risque qu'ils utilisent les données à caractère personnel collectées pour la finalité pour laquelle ils ont été agréés à d'autres fins commerciales. Dans le commentaire des articles, il est précisé que des garanties seront demandées afin d'empêcher cela. Celles-ci feront partie des conditions d'agrément qui doivent être définies par le Roi. La Commission en prend acte et part du principe que le futur arrêté d'exécution susmentionné lui sera encore soumis ultérieurement pour avis. Parallèlement, elle insiste pour que soit déjà repris dans l'avant-projet le principe selon lequel les données à caractère personnel qui sont collectées dans le cadre de l'identification électronique ne peuvent pas être utilisées pour d'autres finalités.

---

[7] Dans le même sens : la Commission a émis un avis favorable dans son avis n° 20/2014 du 19 mars 2014 *concernant le projet d'arrêté royal fixant les conditions, la procédure et les conséquences de l'agrément de services d'identification pour applications publiques numériques qui utilisent des moyens d'identification sans fil* qui rend possible le recours à des services de notification du secteur privé.

38. Le § 5 de l'article 12 de l'avant-projet accorde en outre aux services agréés d'identification électronique une autorisation légale d'utiliser le numéro de Registre national. Toutefois, la nécessité de cette exception légale au règlement repris dans la loi du 8 août 1983 n'est pas motivée. L'article lui-même dispose que le fournisseur d'un service agréé d'identification électronique doit être considéré comme un sous-traitant de l'autorité d'agrément, en l'occurrence Fedict, au sens de l'article 5, premier alinéa, 3° de la loi du 8 août 1983. Cette spécification suffit pour autoriser un tel fournisseur agréé sur la base des dispositions de la loi du 8 août 1983. Il n'y a dès lors aucune raison objective de reprendre une exception à la loi du 8 août 1983 pour ce groupe cible. Il est donc préférable que le texte de ce paragraphe se limite à :

> *"Le fournisseur d'un service agréé d'identification électronique est, pour l'application du présent article, considéré comme un sous-traitant de l'autorité d'agrément au sens de l'article 5, premier alinéa, 3° de la loi du 8 août 1983 organisant un registre national des personnes physiques."*

Par souci d'exhaustivité, la Commission attire l'attention sur le fait que si un fournisseur d'un service agréé d'identification électronique souhaite vérifier des données dans le Registre national en vue de ce service, il devra à cet effet demander une autorisation auprès du comité sectoriel compétent.

Article 13 de l'avant-projet

39. Le premier alinéa de cet article charge le titulaire du MIE d'en prendre soin (contrôle exclusif, protection contre la perte, le vol). Il est précisé dans le commentaire des articles que le contrôle exclusif implique notamment que les mots de passe doivent être tenus strictement confidentiels. La Commission constate que pour un certain nombre de citoyens, il est impossible par exemple de tenir leurs mots de passe strictement confidentiels.

40. De plus en plus de services sont exclusivement accessibles par voie numérique, alors qu'une partie de la population n'a pas pu s'y adapter. Lorsqu'une telle personne souhaite recourir à certains services, elle n'a souvent pas d'autre choix que de remettre par exemple son eID à un tiers et de lui fournir également son code PIN. Le tiers auquel elle a recours sera peut-être une personne qu'elle juge intègre et qui n'abusera donc pas de cet instrument. Qu'en est-il si ce tiers en abuse quand même ? Le titulaire du MIE a-t-il alors été négligent au sens de cet article de l'avant-projet ?

41. Le deuxième alinéa de l'article 13 de l'avant-projet dispose qu'un MIE qui n'est plus valable ou est révoqué ne peut plus être utilisé par le titulaire. Il ressort des explications complémentaires de l'auteur de l'avant-projet du 22 août 2016 qu'il n'est pas inhabituel de responsabiliser le titulaire d'un MIE de cette manière. Le texte révèle que seul le titulaire qui est de mauvaise foi (qui utilise son MIE

tout en sachant que ce dernier est expiré ou révoqué) est visé. La Commission en prend acte et pour être complète, attire l'attention sur le fait qu'une telle responsabilisation du titulaire ne porte évidemment pas préjudice aux obligations et aux responsabilités des autres acteurs (comme le fournisseur du MIE).

PAR CES MOTIFS,
la Commission

émet un avis favorable à condition qu'il soit tenu compte des remarques formulées aux points 5, 13-15, 25-29, 31, 32, 34, 36-38 et 41.

L'Administrateur f.f., Le Président,

An Machtens Willem Debeuckelaere

Centrale drukkerij – Imprimerie centrale